M212924EN-F

Software Installation Guide

IRIS Radar

IRIS and RDA



VAISALA

PUBLISHED BY

Vaisala Oyj
Vanha Nurmijärventie 21, FI-01670 Vantaa, Finland
P.O. Box 26, FI-00421 Helsinki, Finland
+358 9 8949 1
vaisala.com
docs.vaisala.com

© Vaisala 2026

No part of this document may be reproduced, published, or publicly displayed in any form or by any means, electronic or mechanical (including photocopying), nor may its contents be modified, translated, adapted, sold, or disclosed to a third party without prior written permission of the copyright holder. Translated document and translated portions of the document are based on the original English version. Parts of the translation may have been created using machine-assisted translation. In ambiguous cases, the English version is applicable, not the translation.

The contents of this document are subject to change without prior notice.

Local rules and regulations applicable to the products and services may vary, and they shall take precedence over the information contained in this document. Vaisala makes no representations on this document's compliance with the local rules and regulations applicable at any given time, and hereby disclaims any and all responsibilities related thereto. You are instructed to confirm the applicability of the local rules and regulations and their effect on the intended use of the products and services.

This document does not create any legally binding obligations for Vaisala towards customers or end users. All legally binding obligations are set forth exclusively in the applicable contract or in the relevant set of General Conditions of Vaisala (vaisala.com/policies).

This product contains software developed by Vaisala or third parties. Use of the software is governed by license terms and conditions included in the applicable contract or, in the absence of separate license terms and conditions, by the General License Conditions of Vaisala Group.

This product may contain open-source software (OSS) components. In the event this product contains OSS components, then such OSS is governed by the terms and conditions of the applicable OSS licenses, and you are bound by the terms and conditions of such licenses in connection with your use and distribution of the OSS in this product. Applicable OSS licenses are included in the product itself or provided to you on any other applicable media, depending on each individual product and the product items delivered to you.

Table of contents

1. About this document 7
1.1 Version information 7
1.2 Related documents 8
1.3 Documentation conventions 8
1.4 Trademarks 8

2. Security 9
2.1 Password policy 9
2.2 CIS server hardening actions 10

3. File system hierarchy tree 12

4. Preparing for installation 14
4.1 Hardware recommendations 14
4.2 Installation image options 14

5. Installing IRIS/RDA with Kickstart 16
5.1 Creating installation media 16
5.1.1 Creating USB installation media on Windows 16
5.1.2 Creating USB installation media on Linux (AlmaLinux) 17
5.2 Enabling Secure Boot and UEFI boot 17
5.3 Running the installation with Kickstart 18
5.4 First login and password change 21
5.5 Enrolling MOK 21
5.6 Enabling login as root for using IRIS Focus 22
5.7 Verifying that the services are running 23
5.8 Configuring IRIS license setups 24

6. Installing IRIS/RDA software (standalone) 27
6.1 IRIS/RDA installation overview 27
6.2 Logging in as root 27
6.3 Mounting the installation media 27
6.4 Opening a terminal window 29
6.5 Running the installation script 29
6.6 First login and password change 31
6.7 Verifying that the services are running 31

7. Upgrading IRIS and RDA software 33
7.1 Migrating IRIS RDA from older version than 10.x 33
7.2 Upgrading IRIS from 10.0.0 35
7.3 Upgrading IRIS from 10.1 onwards 35
7.3.1 Preparing for the upgrade 36
7.3.2 Getting upgrade software 37
7.3.3 Running the upgrade script 38
7.4 Running Setup after upgrade 39
7.4.1 Invoking Setup and built-in error checking 39
7.5 Checking the kernel module status 42

8. Configuration 43
8.1 Configuring passwords 43
8.1.1 Changing password policy 43
8.2 Configuring RDA software 44

8.3 Configuring firewall....45
8.3.1 Configuring the firewall....45
8.3.2 Configuring the IFDR10 interface....46
8.3.3 Radar cabinet interface....47
8.3.4 Remote IRIS menu interface....47
8.4 Configuring SSH....48

9. Installing IO-62 firmware....49

10. Installing RVP10 (RDA) firmware....51

11. Login, logout, and shutdown....55
11.1 Powering up....55
11.2 Local and remote login....55
11.3 Default usernames and passwords....55
11.4 Running commands with root privileges....55
11.5 Local login as operator after powerup....56
11.6 Powering off....56

12. Troubleshooting....57
12.1 Correcting file ownership and protection....57
12.2 Authorizing remote X–Windows on your node....57
12.3 Making Quick Look Windows (QLW) appear....58
12.4 Replacing failed OS RAID disks....59

Appendix A: Installing AlmaLinux....62
A.1 Overview to installing AlmaLinux....62
A.2 Creating installation media....62
A.2.1 Creating USB installation media on Windows....62
A.2.2 Creating USB installation media on Linux (AlmaLinux)....64
A.3 Installing AlmaLinux automatically....64
A.4 Installing AlmaLinux manually (interactive)....70
A.4.1 Booting the system for manual installation....70
A.4.2 Configuring the system and network....72
A.4.3 Partitioning the destination disk....77
A.4.4 Starting the installation....84
A.4.5 Disabling monitor negotiation....84
A.4.6 Configuring time sync with chronyd....85
A.4.7 Rebooting the system....86
A.4.8 Logging in with your user account....86

Appendix B: IRIS Diagnostic Utilities....87
B.1 ps_iris command....87
B.2 show_iris command....88
B.3 sigmet_env Command....90

Appendix C: Alternative Configurations....92
C.1 Defining the operator list in the startup file....92
C.2 Configuring remote desktop....92

Warranty....95

Technical support....95

Recycling....95

List of tables

Table 1 Related documents (English)....8
Table 2 Password policy based on CIS recommendations....9
Table 3 Manual remediation - vulnerabilities identified and actions taken....10
Table 4 Excluded recommendation....11
Table 5 RDA configuration tools....44
Table 6 Recommended disk partitioning....77

1. About this document

1.1 Version information

This document provides information for system administrators about installing and upgrading IRIS RDA software.

Familiarity with operating system concepts is required.

Document code	Date	Description
M212924EN-F	June 2026	Updated for IRIS RDA 10.5. Updates include: • Updated chapter Creating USB installation media on Windows (page 16). • Added chapter Enabling Secure Boot and UEFI boot (page 17) • Updated chapter Running the upgrade script (page 38) with instructions for updating Kvaser drivers. • Added chapter Enrolling MOK (page 21). • Added chapter Configuring remote desktop (page 92).
M212924EN-E	January 2026	Updated for IRIS RDA 10.4. Updates include: • Added a new chapter about cyber security:Security (page 9). • Password policy is now stricter. Password policy (page 9). • Updated chapter Disabling monitor negotiation (page 84). • Updated instructions for installing AlmaLinux. IRIS RDA is now compatible with AlmaLinux 9 and AlmaLinux 10.
M212924EN-D	June 2025	Updated for IRIS RDA 10.3.0 Updates include: • Updated instructions for upgrading IRIS RDA and AlmaLinux • Corrected command for creating a directory in step 2 in Configuring SSH (page 48) • In chapter *Configuring firewall*, added that by default, the IRIS server firewall is configured so that the NTP service is allowed from the outside network.
M212924EN-C	February 2025	Updated for IRIS RDA 10.2.0 Updates include: • Recommendations for server computer were added. See Hardware recommendations (page 14). • Corrections to commands in Remote IRIS menu interface (page 47) • Notification conventions updated according to the ANSI Z535.6 standard. See Documentation conventions (page 8).

1.2 Related documents

Table 1 Related documents (English)

Document code	Name
DOC236879	*IRIS RDA Release Notes*
M212924EN	*IRIS and RDA Software Installation Guide*
M212925EN	*IRIS and RDA Utilities Guide*
M212926EN	*IRIS Radar User Guide*
M212927EN	*IRIS Programming Guide*
M212928EN	*IRIS Product and Display Guide*
M212923EN	*Radar Control Processor RCP8 User Guide*
M212604EN	*RVP10 Digital Receiver and Signal Processor User Guide*

1.3 Documentation conventions

NOTICE! Alerts you to a situation that, if not avoided, could result in the product to be damaged, or important data to be lost.

Highlights important information on using the product.

Gives tips for using the product more efficiently.

1.4 Trademarks

IRIS™ is a trademark of Vaisala Oyj.

AlmaLinux™ is a trademark of AlmaLinux OS Foundation.

Linux® is a registered trademark of Linus Torvalds.

All other product or company names that may be mentioned in this publication are trade names, trademarks, or registered trademarks of their respective owners.

2. Security

IRIS RDA software has been developed to be compliant with the EN18031-1 Radio Equipment Directive (RED2). As part of this process, the cyber security of the servers used in Vaisala weather radars has been analyzed and enhanced.

For enhancing the security of servers, Vaisala performs server hardening based on the CIS (Center for Internet Security) server hardening script. For reference, the CIS server hardening script is available for subscribed customers at https://workbench.cisecurity.org/.

For details about the server hardening actions, see CIS server hardening actions (page 10).

Besides the server hardening, security hardening of other essential network-capable weather radar components is performed.

Starting in 10.4, Vaisala implements a stricter password policy according to the recommendations by Center for Internet Security (CIS). After the first logins, IRIS RDA system enforces the changing of passwords. See Password policy (page 9).

NOTICE! It is possible to make changes to the password policy, but for security reasons, it is strongly recommended NOT to introduce a less strict policy.

2.1 Password policy

At the server installation, CIS hardening is done and password policy rules are enforced accordingly. The password policy is based on the recommendations given by Center for Internet Security (CIS).

Table 2 Password policy based on CIS recommendations

Item	Default rule
Password length	Minimum: 14 characters
Password quality	Minimum: characters from 4 classes • letters in upper case • letters in lower case • digits • other characters
Maximum number of consecutive characters	3
Maximum number of sequential characters	3
No cracklib dictionary words	
Password expiration time	365 days

2.2 CIS server hardening actions

As part of the implementation of the Radio Equipment Directive (RED2), the cyber security of the servers used in Vaisala radars has been analyzed and enhanced. This chapter describes the identified vulnerabilites and actions to mitigate them.

Actions for mitigating vulnerabilities in IRIS RDA software

The vulnerabilities listed in the following table were identified in IRIS RDA software, and actions to mitigate them were taken according to the recommendations given by CIS.

Table 3 Manual remediation - vulnerabilities identified and actions taken

ID (Radio Equipment Directive RED2)	Action to mitigate a vulnerability
1.2.1.1	Ensure GPG keys are configured.
1.4.1	Set bootloader password.
1.6.6	Ensure system wide crypto policy disables `chacha20-poly1305` for ssh.
1.6.7	Ensure system wide crypto policy disables `EtM` for ssh.
2.1.22	Ensure only approved services are listening on a network interface.
4.2.1	Ensure `firewalld` drops unnecessary services and ports.
5.1.7	Ensure `sshd` access is configured.
6.1.2	Ensure that file system integrity is regularly checked.
6.2.1.2	Ensure `journald` log file access is configured.
6.2.2.2	Ensure `journald ForwardToSyslog` is disabled.
6.2.4.1	Ensure access to all log files has been configured.

Security enhancements to other radar system components

In addition to the radar server hardening, other network-capable devices in the Vaisala weather radar systems were checked. Based on the RED2 analysis, the following actions were taken:

- Remove cockpit service installation
- CAN-Ethernet interface hardening
- Cibred dehydrator hardening
- Moxa Serial-Ethernet interface hardening
- Documenting exposed NTP service/port in customer documentation
- Guiding customers to change the radar server passwords during site acceptance tests

Excluded recommendations

The following table lists the recommendations where actions were not taken and the reasons for this.

Table 4 Excluded recommendation

ID (RED2)	Recommendation	Reason for exclusion
1.1.1.8	Ensure usb-storage kernel module is not available.	USB storage file system needed for IRIS/RDA update.
1.1.1.9	Ensure unused file systems kernel modules are not available.	No unused file system kernel modules.
2.1.12	Ensure `rpcbind` services are not in use.	IRIS remote menu is using `rpcbind`.
4.2.2	Ensure `firewalld` loopback traffic is configured.	IRIS/RDA uses loopback for communication.
7.1.11	Ensure world writable files and directories are secured.	Postponed until for future release due to technical reasons.

3. File system hierarchy tree

```
├── etc
│   ├── vaisala
│   │   └── irisrda
│   │       ├── images
│   │       ├── init
│   │       ├── listings
│   │       ├── menu
│   │       └── overlay
│   │   └── irisrda_templates
│   ├── systemd /* service files */
│   ├── profile.d /* shell script files */
│   ├── rc.d
│   │   └── init.d /* rc files */
│   └── logrotate.d /* logrotate conf files */
├── srv
│   └── iris_data
│       ├── ingest       /* IRIS ingest files */
│       ├── product      /* IRIS derived product files */
│       ├── product_raw  /* IRIS RAW (packed ingest) files */
│       ├── tsarchive    /* saved IQ data */
│       ├── tape_inv     /* tape backup metadata */
│       ├── ascope     /* Data saved from ascope utility */
│       ├── suncal     /* Sun based calibration utility data */
│       ├── temp       /* temp storage */
│       └── zdrcal     /* ZDR calibration utility data */
├── usr
│   ├── libexec
│   │   └── vaisala
│   │       ├── pipes /* pipes from data_converters */
│   │       └── irisrda /* scripts for irisrda */
│   ├── bin /* executables for irisrda */
│   ├── share
│   │    ├── X11 /* app defaults resource files */
│   │    ├── nls /* po files */
│   │    ├── vaisala
│   │    │   └── irisrda
│   │    │       ├── icons /* icon files */
│   │    │       ├── sounds /* sound files */
│   │    │       └── keys /* key files */
│   │    └── doc /* user documentation, release notes and license files */
│   ├── lib64 /* all libraries */
│   └── include
│        └── vaisala/* all header files */
```

```
└── var
    ├── log
    │   └── irisrda /* all log files */
    └── spool
        └── vaisala-io
            ├── input      /* Default IRIS input directory */
            ├── output     /* Default IRIS output directory */
            ├── raw
            ├── volume
            └── temp       /* Conversion pipes temp storage */
```

4. Preparing for installation

4.1 Hardware recommendations

Vaisala recommends using a server computer that meets the following spesifications:

Feature	Recommendation
Drive size	512 GB SDD configured with RAID 1 (mirrored)
Memory	16 G of DDR4 Memory
CPU	2 XEON E5-2609 v3 Processors with 6 Cores, 1.9 GHz clock speed, 6.4GT/s QPI Speed, 15M of Cache

The server provided by Vaisala meets these recommendations.

4.2 Installation image options

This version of IRIS RDA software can be run on AlmaLinux 9 or AlmaLinux 10.

Vaisala provides customized ISO images for AlmaLinux and IRIS/RDA software on the Vaisala FTP website:

https://ftp.sigmet.vaisala.com/files/releases.

For each, two options are available: AlmaLinux 9.7 and AlmaLinux 10.1.

ISO Image	Notes	Instructions
Combined AlmaLinux OS and IRIS/RDA sw ISO image	Automatically installs both the AlmaLinux operating system and the IRIS/RDA software. Available on USB drive and FTP site. You can also use this image to only install the IRIS/RDA software.	Installing OS together with IRIS/RDA: Chapter *Installing IRIS/RDA and AlmaLinux with Kickstart* Installing only IRIS/RDA: Chapter *Installing IRIS/RDA software*
IRIS/RDA software as standalone ISO image	This image is smaller than the combined ISO image, so it is faster to download. Available on the FTP site.	Chapter *Installing IRIS/RDA software*
AlmaLinux operating system as standalone ISO image	This image is smaller than the combined ISO image, so it is faster to download. Available on the FTP site.	Appendix *Installing AlmaLinux*

When installing the IRIS/RDA standalone ISO, you can select either online or offline installation. The online option enables access to RPMs from remote repositories that are needed if the host system does not contain dependencies that come from `AppStream` and `BaseOS` repositories. These repositories are automatically included when the combined OS and software ISO image used. The online installation requires Internet connection.

If you select the offline installation option, the installation only uses the repositories provided by ISO image and does not try to access remote repositories. In this case, for example, `devel` packages cannot be installed, because they require a specific version of base packages and this requires accessing remote repositories.

5. Installing IRIS/RDA with Kickstart

5.1 Creating installation media

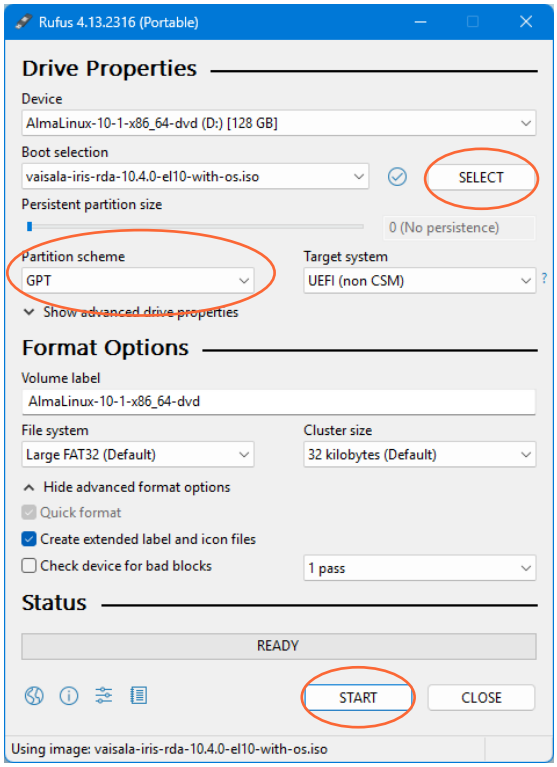
Start the installation process by creating and initializing the installation media.

5.1.1 Creating USB installation media on Windows

These instructions apply to Windows 10 and Windows 11.

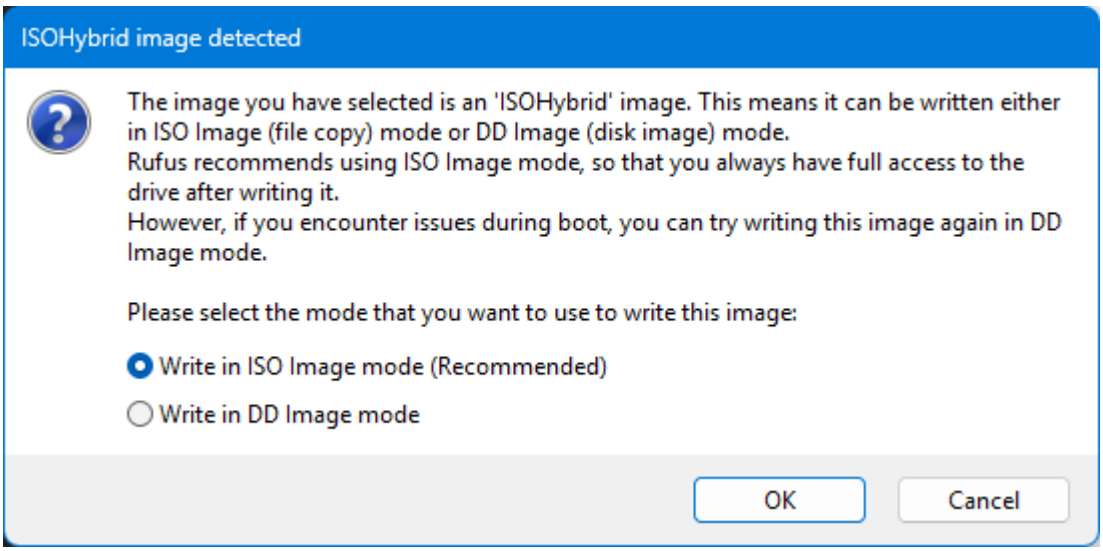
When creating USB installation media on Windows, use a standalone program such as `Rufus` (available at http://rufus.akeo.ie/). Follow the on-screen instructions.

1. Launch `Rufus` by double-clicking the program icon.
2. Insert a USB drive in the USB port.
3. In the `Rufus` window, click **Select**, and select the iso image.
4. In the **Partitition scheme** drop-down menu, select **GPT**.
5. Select **START**.



6. When the **ISOHybrid image detected** pop-up window opens, select **Write in ISO Image mode**.

7. Select **OK**.



8. If the program asks for a permission to find a `grub2` bootloader online, reply **`Yes`**.
9. When the USB media is ready, select **Close**.

5.1.2 Creating USB installation media on Linux (AlmaLinux)

> **NOTICE!** This operation destroys data on the device you operate on.

1. Run **`$ lsblk`** to list block devices on your system. Take note of the output.
2. Insert a USB drive in the USB port.
3. Run **`$ lsblk`**.

   Compare the output to the previous step. The additional block device from this output is your USB drive.
4. Run **`$ dd if=path/toAlmalinux.iso of=/dev/xxx`**

   Where */dev/xxx* is the path to the USB drive. Do not use the partition number for the USB drive.
   For example: */dev/sdc*.

5.2 Enabling Secure Boot and UEFI boot

Before installing AlmaLinux, enable Secure Boot and UEFI boot in BIOS settings.

The procedure below describes how to do this on the RVP10SRV server.

The procedure below only describes how to set the Secure Boot and UEFI boot in the RVP10SRV server delivered by Vaisala. If you have a different server, the procedure is likely to be different. See server manufacturer's documentation for instructions.

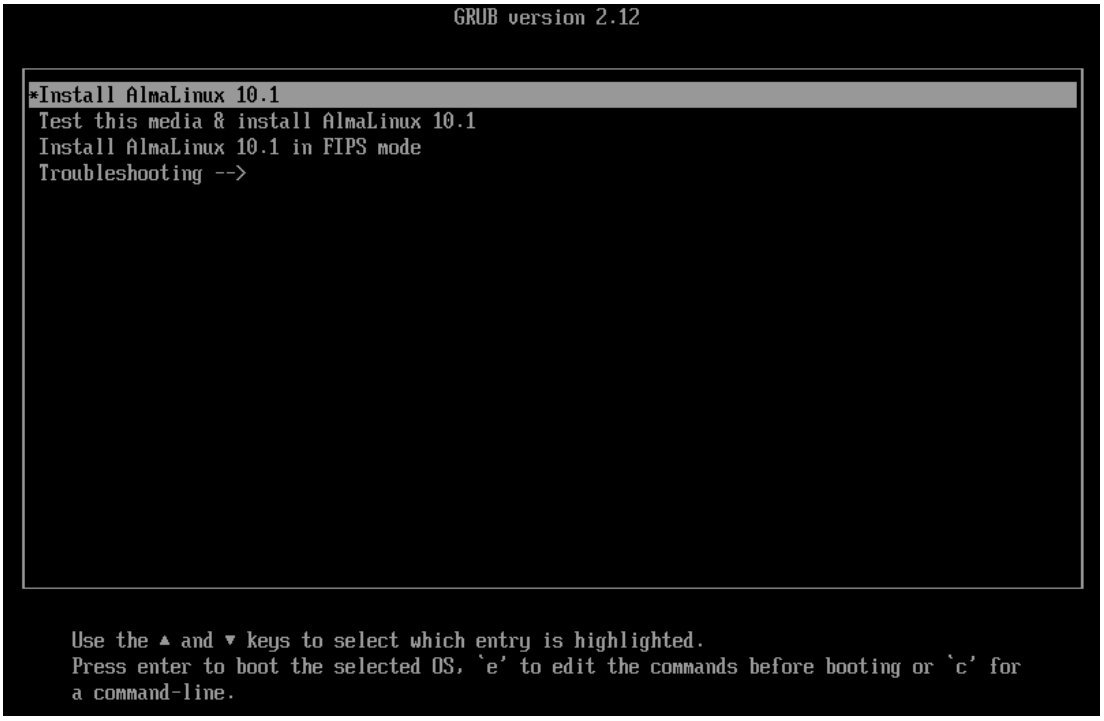
1. Insert the installation media in the server.
2. **Enable Secure Boot:**
   a. Hold down the **Delete** key and power up the system. Keep the **Delete** key pressed down until the BIOS setup is opened.
   b. Use the arrow keys to highlight the **Advanced** option at the top of the window. Use the arrow keys to highlight **CSM Configuration** and press **Enter**.
   c. Change the **CSM Support** status to **Disabled**.
   d. Press **F4**, select **Yes**, and press **Enter** to save the setup and reboot.
   e. After reboot, hold down the **Delete** key while powering up the system. Keep the **Delete** key pressed down until the BIOS setup is opened.
   f. Use the arrow keys to highlight the **Security** option at the top of the window. Use the arrow keys to highlight **Secure Boot** and press **Enter**.
   g. Change the **Secure Boot** status to **Enabled**.
   h. Use the arrow keys to highlight **Restore Factory Keys** and press **Enter**.
   i. Press **F4**, select **Yes**, and press **Enter** to save the setup and reboot.
3. **Enable UEFI boot:**
   a. After reboot, hold down the **Delete** key while powering up the system. Keep the **Delete** key pressed down until the BIOS setup is opened.
   b. Use the arrow keys to highlight the **Save & Exit** option at the top of the window.
   c. In the **Save & Exit** screen, under the **Boot Override** title, select the **UEFI: Asolid USB** media that you will be installing from and press **Enter**.
   d. Press **F4**, select **Yes**, and press **Enter** to save the setup and reset.

5.3 Running the installation with Kickstart

You can select between the AlmaLinux 9.7 and AlmaLinux 10.1. Kickstart versions. This chapter uses AlmaLinux 10.1 as the example.

1. In the AlmaLinux window, select **Install AlmaLinux 10.1**, and press **Enter**.

> **NOTICE!** Do not use the option **Test this media & install AlmaLinux 10.1**. It skips the configuration process.



2. When prompted, configure the hostname and IP address.

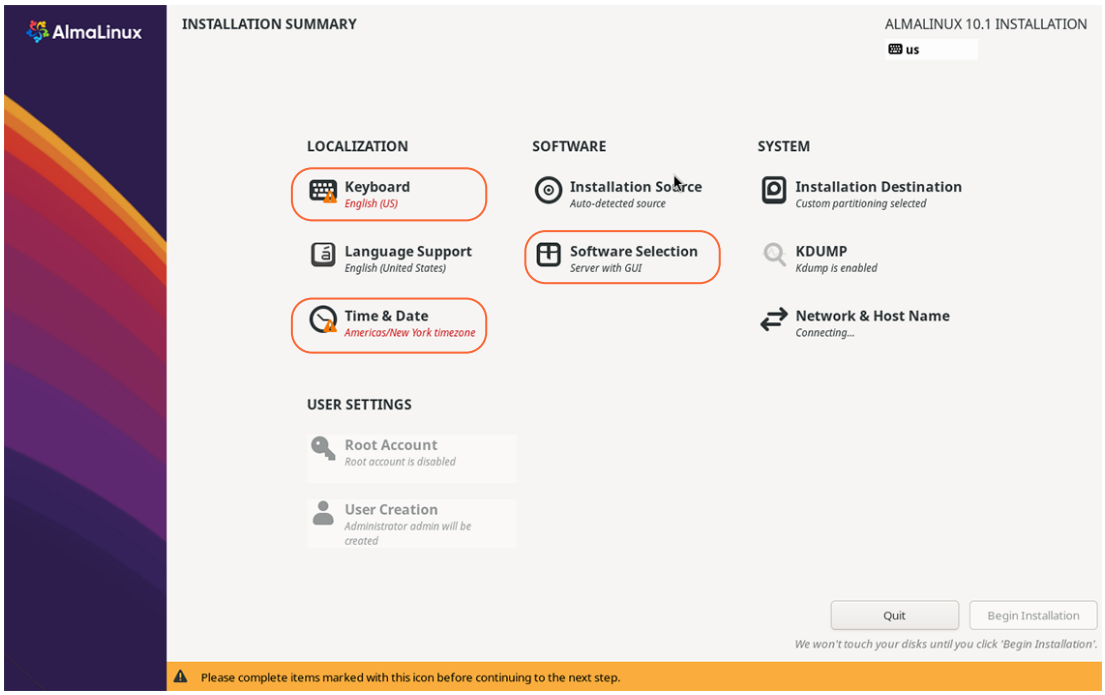
```
Enter Hostname: new-radar


======= Configuring for enp0s3 =======
Do you want to configure this interface? [y/n] y
Configure as static (default is DHCP)? [y/n] n

======= Configuring for enp0s8 =======
Do you want to configure this interface? [y/n] y
Configure as static (default is DHCP)? [y/n] y
Enter IP address: 10.0.2.1
Enter netmask: 255.255.255.0

======= Configuring for enp0s9 =======
Do you want to configure this interface? [y/n] y
Configure as static (default is DHCP)? [y/n] y
Enter IP address: 10.0.3.1
Enter netmask: 255.255.255.0
```

3. In the **Installation Summary** window:



a. Select **Keyboard** and select the desired keyboard version.
b. Select **Time & Date** and set the time and date.
c. Select **Software Selection**.

4. In the **Software selection** window, select **Server with GUI** and the software you want to install.

   By default, **IRIS**, **RCP8**, **RVP10**, **AIDE**, and all data converter RPMs are selected. For more information on the options, see Running the installation script (page 29). **AIDE** is a tool used in server hardening. If selected, it is formatted during the installation process, so that you can take it into use later (it is not taken into use automatically).

5. In the **Installation Summary** page, select **Begin Installation**.

   The installation process begins.

6. When the installation is complete, the system will reboot automatically.

5.4 First login and password change

The IRIS RDA software installation creates three default user accounts: **radarop**, **observer**, and **admin**.

After installing IRIS RDA from installation media, the default password is **xxxxxx**. Changing this password on the first login is mandatory.

> **NOTICE!** If you do not change the **xxxxxx** password, you will be locked out of the system.

1. After the login window opens, wait for about 3 minutes for the server hardening to get ready.

   As part of the server hardening, after about 3 minutes, the login icons for the various users disappear. After this, you have to type in the username (**radarop**, **observer**, or **admin**) in the login window.

2. Enter the default password.
3. Change the password.
4. Do the same for the other default user accounts (**observer** and **admin**).

More information

- Password policy (page 9)

5.5 Enrolling MOK

For the akmods built kernel modules to work with Secure Boot, perform the akmods MOK (machine owner key) enrollment. The **mokutil** tool is used for this.

1. Log in as `admin`.

2. Open the terminal window and type:

```
$ sudo mokutil --import /etc/pki/akmods/certs/public_key.der
```

   The **mokutil** tool starts.
3. When prompted, type the admin password.
4. Set a temporary MOK enrollment password:
   a. For the prompt **Input password:**, type in the temporary password **`vaisala`** and press **Enter**.
   b. Repeat the password.

   Now you have set the password for MOK enrollment. You will need this password also later in the process.
5. Reboot the server by typing:

```
reboot
```

6. When AlmaLinux is restarting again, it prompts for the MOK enrollment. When you see the text **Press any key to perform MOK management**, press any key in the keyboard promptly before the short timer runs out.
7. In **MOK Management**, select **Enroll MOK** and press **Enter**.
8. In the **Enroll MOK** screen, select **Continue** and press **Enter**.
9. In the **Enroll the key(s)?** screen, select **Yes** and press **Enter**.
10. Type in the MOK enrollment password **`vaisala`**.
11. In the **Perform MOK management** screen, select **Reboot** and press **Enter**.
12. Wait for the server to reboot.
13. Log in as **`admin`**.
14. Open the terminal window and type:

```
$ sudo akmods --rebuild --force
```

    Wait until all kernel modules are rebuilt. This takes few minutes.

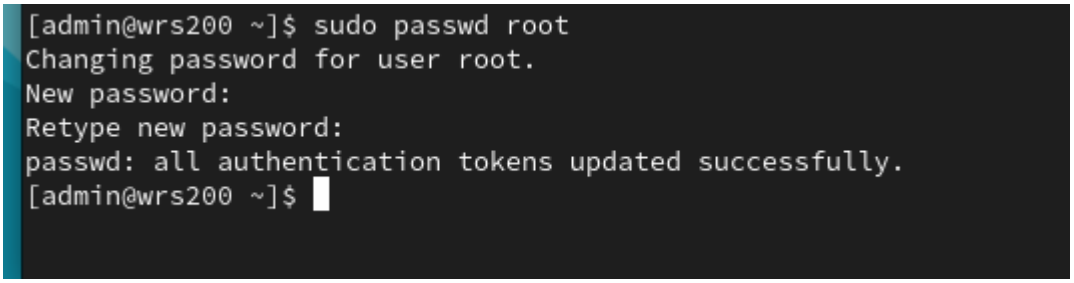
5.6 Enabling login as **`root`** for using IRIS Focus

If you are installing IRIS Analysis and IRIS Focus on the same server, you need to enable logging in as **root**.

1. Log in as **admin** user.
2. Type:

```
$sudo passwd root
```

3. Follow the prompts.



4. Log out, and log in as **root**.

5.7 Verifying that the services are running

1. If you have not done so already, log in as **radarop**.
2. In the terminal window, list the services currently running by typing:

```
# ps_iris
```

The **COMMAND** column lists the running services.

Option	Running services
-rvp10	rvp10
-rcp8	rcp8

You may also see that the antenna (**ant_***) and receive (**rtd_***) processes have started.



IRIS does not start until you have installed the IRIS license.

More information

- ps_iris command (page 87)

5.8 Configuring IRIS license setups

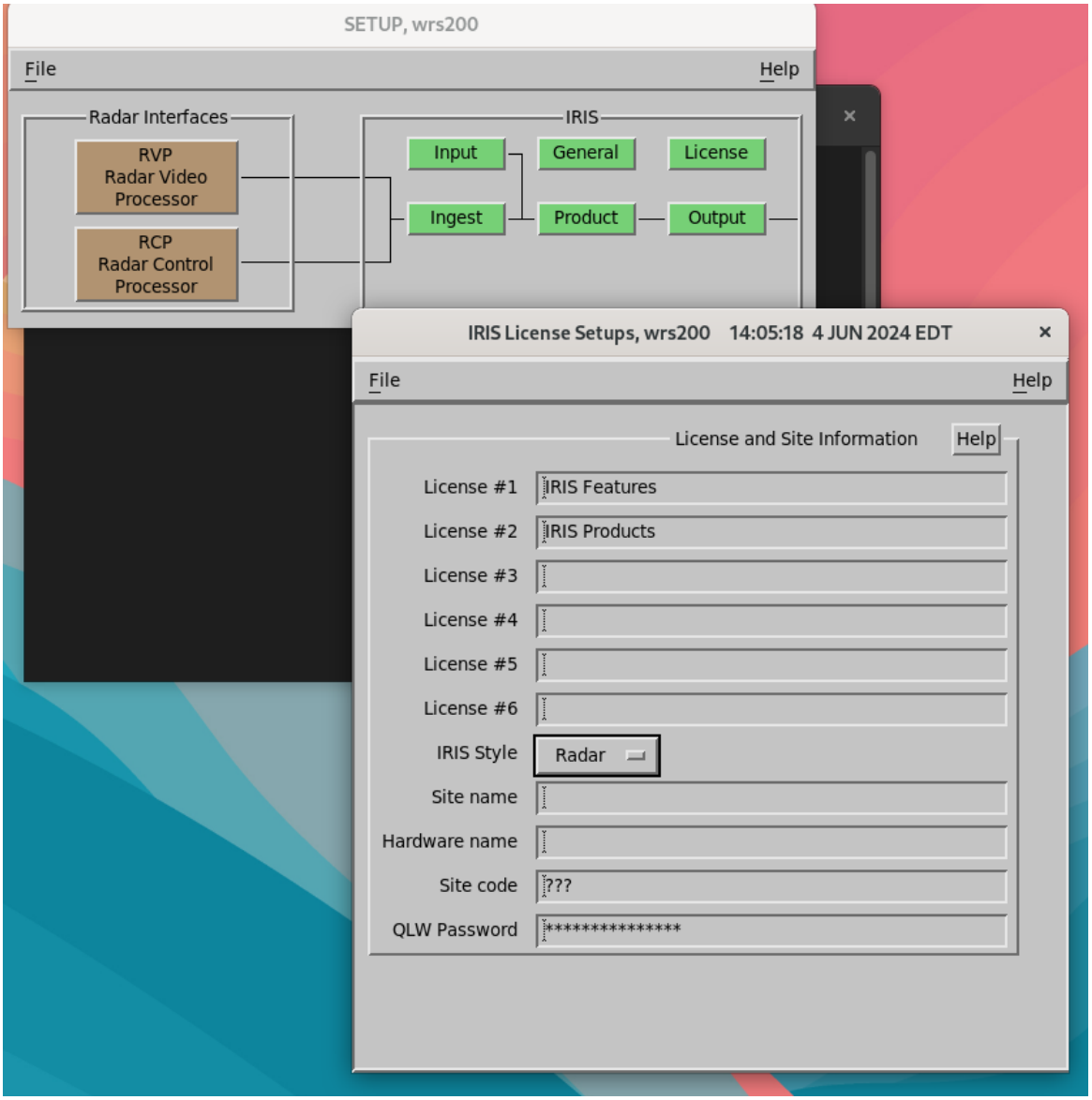


Figure 1 License setup example

Before you can use IRIS/RDA software, you must request and set up a license.

1. Open the **Setup** utility by typing:

```
setup&
```

2. In the **Setup** utility, select **License**.
   a. Delete the default texts in the **License** fields.
   b. Depending on your setup, for **IRIS Style**, select either **Radar** or **Analysis**.
   c. In **Site name**, type a name for the machine (typically the host name of the machine).

      For example: **`hel-radar`**
   d. In **Site code**, type a code name for the radar site.

      For example: **`HEL`**
   e. In the **IRIS License Setups** window, select **File > Close**
   f. Select **File > Save** and **File > Exit**.
3. In the terminal window, type: **`show_machine_code`**

   The terminal prints the licensing information about this machine. For example:

```
-------------------------------------------------
Licensing Information for IRIS Version 10.4.0
-------------------------------------------------

Machine Code: EMNTRK
Site Name: hel-radar
Check Code: WPEFXE
OS Name: Linux
OS Release: 3.10.0-229.el7.x86_64
Host Name: localhost.localdomain
Locking To: host
```

4. Copy all the information under `Licensing Information for IRIS Version <version number>`
5. Contact your Vaisala representative and request an IRIS license.

   Provide the information you copied in the previous step.
6. When you receive the license from Vaisala, return to **Setup > License** and type the **License 1**, **License 2**, ... license codes *in the order listed in the license*.

   Depending on your configuration, you may have codes such as:
   - IRIS Features Code
   - IRIS Product Code
   - RDA Features Code
7. Select **File > Save** and **File > Exit**.

8. To confirm that your license is correctly setup, start IRIS by typing:

```
siris
```

Check that the IRIS **Quick Look Window** starts.
If the IRIS **Quick Look Window** does not start, see Troubleshooting instructions.

6. Installing IRIS/RDA software (standalone)

6.1 IRIS/RDA installation overview

Installing the IRIS/RDA software from the installation media with a script involves the following steps. The steps are described in detail in the following chapters.

1. Install the AlmaLinux operating system according to Appendix *Installing AlmaLinux*.
2. Log in as **`root`**.

   See Logging in as root (page 27).
3. Install the IRIS / RDA installation media, and verify that it mounts.

   See Mounting the installation media (page 27).
4. Open a terminal window.
5. Run the installation script.
6. Verify that the expected services have started.

   See Verifying that the services are running (page 23).
7. Configure your licenses.

   See Configuring IRIS license setups (page 24).
8. Check and update your firmware as needed:
   - Installing IO-62 firmware (page 49)
   - Installing RVP10 (RDA) firmware (page 51)

6.2 Logging in as root

1. Enter **`root`** as the user name and your root password.

   The system displays a welcome message after the first time you log in and a blank screen after other logins.
   If prompted, select your language and input settings.

You can now continue with the IRIS RDA software installation.

6.3 Mounting the installation media

The IRIS/RDA installation media can be either a USB drive or a DVD disc.

1. Log in as **admin**.
2. Insert the USB drive in the USB port of the server, or insert the DVD disc in the DVD drive.

3. Depending on your AlmaLinux installation, the installation media may be automounted. Follow the **Automount** procedure if it is, or the **Manual mounting** procedure if it is not.
4. **Automount:**
   a. A small black window indicates that the installation media has been recognized.

      Select **X** in the upper right corner to close the window.

   b. Verify that the installation media is mounted by typing:

      ```
      df -h
      ```

      The installation media should be listed with the mount point in */run/media/root/irisrda_X.XX.X*, where `X.XX.X` is the version of software you are installing.
5. **Manual mounting:**

   If the installation media is not automounted or not visible in `df -h`, mount it manually:

   a. List available devices with the command:

      ```
      lsblk
      ```

      The output lists the available storage devices and partitions. Identify the device corresponding to your installation media (for example, `/dev/sdb1`).

   b. Create a mount point directory, if it does not yet exist (replace `<device>` with a suitable name for your installation media, such as `irisrda`):

      ```
      sudo mkdir -p /mnt/<device>
      ```

   c. Mount the installation media to the created path (replace `<device-node>` with the device from the `lsblk` list, for example `/dev/sdb1`):

      ```
      sudo mount <device-node> /mnt/<device>
      ```

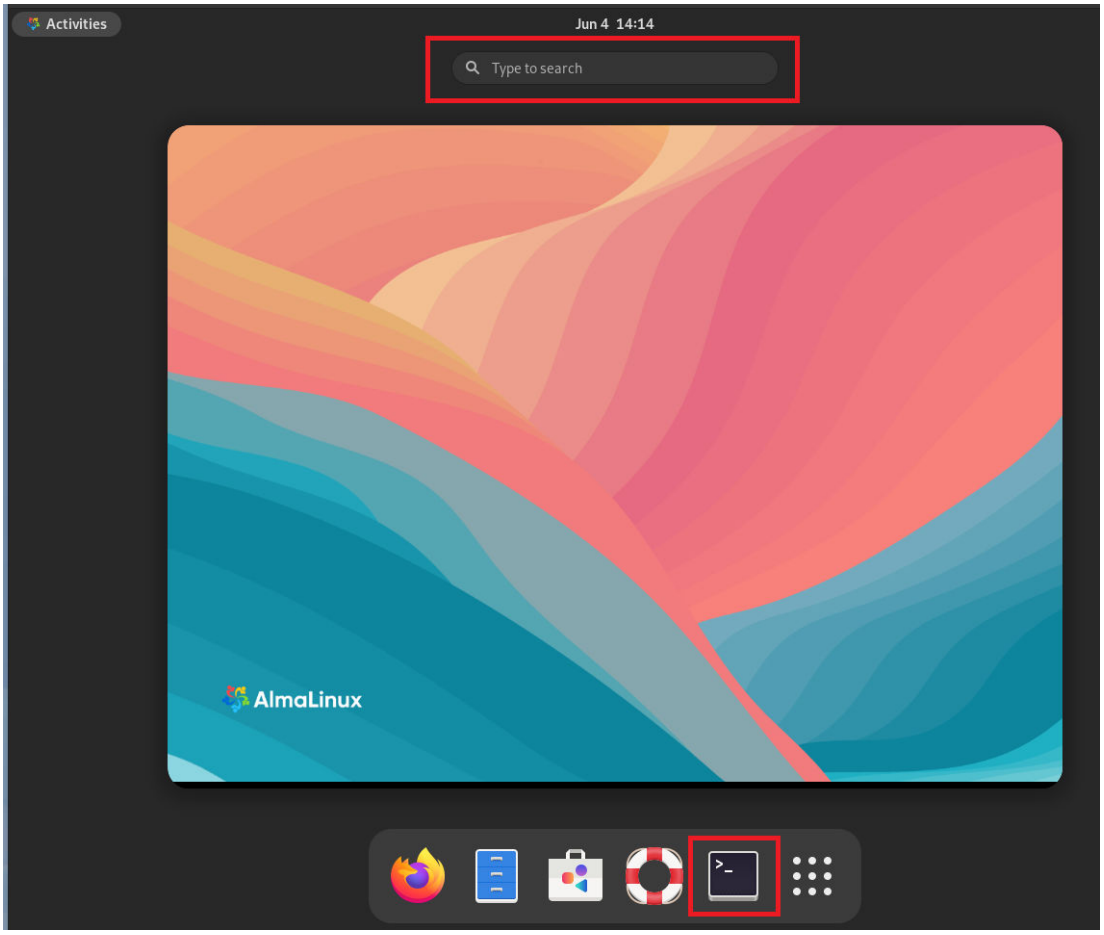
6. To verify that the installation media is accessible, list its contents (replace `<device>` with the name you used above):

   ```
   ls /mnt/<device>
   ```

   You should see the files and directories from the installation media.

6.4 Opening a terminal window

1. In the upper left corner, left-click **Activities**.
2. Either type **`terminal`** in the search field on top of the window, or click on the terminal icon at the bottom of the screen.



A terminal window with a prompt opens.

3. Remove the user you created during the operating system installation.

   For example, if you created the user **`service`**, type:

```
# userdel -r service
```

6.5 Running the installation script

The *`vaisala-iris-rda-install.sh`* script automatically performs all the processes the make the system ready to run. For example, the script installs the requested products with their dependencies, creates directories, and configures paths and users.

The script also sets up a local repository that is required for installing upgrade packages via DNF.

1. Change to the directory where the IRIS/RDA installation media is mounted.

   For example, if the mounting point is */run/media/root/irisrda*, type:

   ```
   # cd /run/media/root/irisrda
   ```

2. Run the installation script with desired parameters by typing:

   ```
   ./vaisala-iris-rda-install.sh <parameter>
   ```

   , where **<parameter>** can be any of the following:
   - `--help`: Prints out the applicable parameters.
   - `--iris`: Installs IRIS on a running system (with all dependencies, including **common** package).
   - `--rcp8`: Installs RCP8 on a running system (with all dependencies, including **common** and **rda** packages).
   - `--rvp9`: Installs RVP9 on running system (with all dependencies, including **common** and **rda** packages).
   - `--rvp10`: Installs RVP10 on a running system (with all dependencies, including **common** and **rda** packages).

     `--rvp9` and `--rvp10` options cannot be used at the same machine.

   - `--converter "<converter_name> <converter_name> <converter_name> ..."`: Installs **data-converters-<converter_name>** on running system (with all dependencies, including **common** package). Accepts converter list inside quotes as argument.
     The option `--help` shows all converter names that can be installed with the script.
   - `--online`: provides access to remote repositories that is set up on system.
   - `--offline`: forces the script to use the repositories provided by the ISO image. No access to remote repositories.
   - `--with-os`: If you want to point the external DVD ISO for dependencies that come from AppStream and BaseOS, provide the mount path of the AlmaLinux DVD. Providing `--os-media` may be useful if third party dependencies are not already installed on your system and installation image does not include those dependencies when you are running the offline installation.

3. Reboot the system to apply changes and to run enabled services:

```
reboot
```

6.6 First login and password change

The IRIS RDA software installation creates three default user accounts: **radarop**, **observer**, and **admin**.

After installing IRIS RDA from installation media, the default password is **xxxxxx**. Changing this password on the first login is mandatory.

> **NOTICE!** If you do not change the **xxxxxx** password, you will be locked out of the system.

1. After the login window opens, wait for about 3 minutes for the server hardening to get ready.

   As part of the server hardening, after about 3 minutes, the login icons for the various users disappear. After this, you have to type in the username (**radarop**, **observer**, or **admin**) in the login window.
2. Enter the default password.
3. Change the password.
4. Do the same for the other default user accounts (**observer** and **admin**).

More information

- Password policy (page 9)

6.7 Verifying that the services are running

1. If you have not done so already, log in as **radarop**.

2. In the terminal window, list the services currently running by typing:

```
# ps_iris
```

The **COMMAND** column lists the running services.

Option	Running services
`-rvp10`	`rvp10`
`-rcp8`	`rcp8`

You may also see that the antenna (`ant_*`) and receive (`rtd_*`) processes have started.



IRIS does not start until you have installed the IRIS license.

More information

- ps_iris command (page 87)

7. Upgrading IRIS and RDA software

7.1 Migrating IRIS RDA from older version than 10.x

Follow this procedure if you have IRIS/RDA version that is older than version 10 (for example, 9.x).

1. Log in as **root**.
2. Prepare the USB stick for backing up the configuration:

   To identify the USB stick, insert the USB stick into USB port, and list devices by running command:

   ```
   lsblk
   ```

   If necessary, unmount any mount point with the command: `umount /<mountpoint>`.
3. Partition the USB stick:
   a. Run the `fdisk` command, for example:

      ```
      fdisk /dev/sdx
      ```

      where `sdx` was identified in the previous step (identifying USB stick).
   b. Follow the on-screen help to delete, create, and write to save the partition.
   c. Format the USB stick with the command:

      ```
      mkfs.ext4 /dev/sdx1
      ```

      Wait until the command has finished running.
   d. Mount the USB stick with the command:

      ```
      mount /dev/sdx1 /mnt
      ```

4. Save the IRIS/RDA configuration:
   a. Change the directory to */usr/sigmet/config*.
   b. Save the configuration with the command:

```
tar -zcvpf /mnt/config.tgz .
```

   c. Unmount the USB stick with the command:

```
sudo umount /dev/sdx1
```

5. Install IRIS using Kickstart from IRIS ISO image. Follow the normal IRIS installation instruction.

   When IRIS installation has completed, follow the instructions to complete the installation.

6. Restore the IRIS configuration:
   a. Login as **admin**.
   b. Insert the USB stick that has the backup configuration file into the USB port.
   c. Run the **df** command and identify the USB stick mounting point. Change the directory to that mount point.
   d. Restore the configuration with the command:

```
sudo tar -zxvpf config.tgz -C /etc/vaisala/irisrda/
```

7. Modify the IRIS setup:
   a. Edit every *setup_xxx* file in the */etc/vaisala/irisrda/* directory: change the string that refers to */usr/iris_data* to */srv/iris_data/* as root directory.
   b. Replace the directory for output and input device to */var/spool/vaisala-io/* as root directory. Alternatively, run **iris setup**, and modify according to the file system tree (see File system hierarchy tree (page 12)).
   c. Make sure all files and directories in **/etc/vaisala/irisrda** are owned by **operator.users**.

      If not, make correction with the command:

```
sudo chown -R operator:users /etc/vaisala/irisrda/
```

7.2 Upgrading IRIS from 10.0.0

Follow this procedure to upgrade your system if you have IRIS 10.0.0 with AlmaLinux 9.

1. Log in as **admin** user.
2. Change directory to */etc/vaisala*.
3. Run the command:

```
sudo tar -zcvpf path/usbstick
```

4. Follow the steps in Migrating IRIS RDA from older version than 10.x (page 33) to prepare the USB stick.
5. Install IRIS using the Kickstart IRIS ISO image with operating system.
6. After installation, restore the configuration with command:

```
sudo tar -zxvpd path/config.tgz -C /etc/vaisala/
```

7. Make sure all files and directories in */etc/vaisala/irisrda* are owned by **operator.users**.

   If not, make correction with the command:

```
sudo chown -R operator:users /etc/vaisala/irisrda/
```

7.3 Upgrading IRIS from 10.1 onwards

Follow this procedure to upgrade your system if your system has IRIS RDA 10.1 or later version and you want to upgrade it into a newer release.

The upgrade is handled by the DNF package manager installed by the IRIS 10.1 installation script. In the upgrade process, the DNF replaces existing RPMs with new RPMs.

The upgrade process includes the following steps:

1. Back up your configuration files. See Preparing for the upgrade (page 36).
2. Get the latest software release ISO image and *Release Notes* at *https://ftp.sigmet.com/files/releases/*. See Getting upgrade software (page 37).
3. Run the upgrade installation script. See Running the upgrade script (page 38).
4. Run the **Setup** utility. See Running Setup after upgrade (page 39).

7.3.1 Preparing for the upgrade

1. Log in as **root**.

   See Logging in as root (page 27).

2. Back up and save important configuration files.

   As part of the upgrade, many files are erased and replaced. However, the upgrade procedure preserves everything in *${IRIS_CONFIG}*.

   a. Back up and save customized configuration files.

   b. Even though this file is not overwritten during the upgrade, create a backup of */etc/vaisala/irisrda*:

   ```
   # cd /etc/vaisala/
   # tar cfz <config_nodename_date.tgz> irisrda/
   ```

   c. To back up the whole installation (for example, to support rollback), back up */etc/vaisala*:

   ```
   # cd /etc/
   # cp -R vaisala/ sigmet_versionNumber/
   ```

3. Print the current setup.

   Run the **Setup** utility on the old system, and generate an ASCII listing file with the **File/List** command.
   The format of these files can change between software versions, so you may need to re-enter some information.
   A date coded listing file is generated in the *${IRIS_LISTING}* directory, typically in */etc/vaisala/irisrda/listings*.

4. Make sure all applications are stopped by exiting any IRIS/RDA utilities that you are running and typing the command:

   ```
   $ qiris
   ```

5. Verify that all processes have stopped by typing:

   ```
   ps_iris
   ```

6. Stop any running processes as **root** with the **kill <process ID number>** command.

   The process ID number is the first column of numbers from the **ps_iris** output.

7.3.2 Getting upgrade software

New features and updates are provided as software upgrades from the following sources:

- FTP download
  Connect to the Vaisala Sigmet server in ftp.sigmet.vaisala.com.
  - If using a web browser, navigate to */files/releases/<latest version>*
  - If using an FTP client, navigate to */outgoing/releases/latest version>*

  These public releases are free of charge, but do not include support services unless you are under warranty or have purchased a support contract from Vaisala. Contact your Vaisala representative to arrange a support contract.
- USB drive or DVD disc
  Provided as part of a support contract or upon request.

7.3.2.1 Downloading upgrade files

The examples in this procedure use release 10.1.0 as an example. In most cases, you install the most recent version, labelled below as <X.XX>.

1. Create a directory named */tmp/iris-<X.XX>*.
2. If you are downloading RDA software, create a directory named */tmp/rda-<X.XX>*.

   You should make a separate directory for each version and type (IRIS/RDA) of software that you download.
3. Login as **radarop**.

```
$ cd /
$ mkdir /tmp/rda-10.1.0
```

4. Change to the */tmp* directory by typing:

```
$ cd /tmp/rda-10.1.0
```

   On Windows machines, you can type the commands in the command prompt (remember to use the "\" backslash for DOS).

5. Start the FTP browser.

6. In the directory listing of available releases, find your release.
7. Download the *irisrda_image.iso*.

   Download the appropriate software image according to OS version (AlmaLinux 8, AlmaLinux 9).

7.3.3 Running the upgrade script

This instruction assumes that the operating system stays the same.

1. Log in as **admin**.
2. Mount the ISO image:

```
sudo mount -o loop <iso-image> /mnt
```

3. Change the directory to */mnt*:

```
cd /mnt
```

4. Run the command:

```
sudo dnf upgrade -y --allowerasing --nogpgcheck --disablerepo="" \
                    --repofrompath vaisala-local,$(pwd)/vaisala-iris-rda \
                    --repofrompath vaisala-extras-local,$(pwd)/vaisala-iris-
rda-extras \
                    vaisala-wr-* kvasercan-lib
```

5. Remove old Kvaser drivers:

```
sudo dnf remove *kvaser-leaf* *kvaser-mhydra* *kvaser-usbcanII*
```

6. Run the command:

```
sudo akmods
```

7.4 Running Setup after upgrade

After upgrading, the **Setup** utility fills in default values for any new settings that were added. Vaisala recommends reading the *Release notes* document and then checking the new settings to make sure they are right for your system.

1. Login as **radarop**.

   The default password is: **`Va1sala!factory`**
   (Note that the first character is capital letter '**V**', and the third character is number one '**1**'.)

2. Launch the **Setup** utility.

   At startup for an upgrade, **Setup** checks the parameters to verify that they are within reasonable bounds and lists any problems.
   The listing gives the name of the variable in question and prompts the user to consider the repair command. Errors are usually related to new features that have not been addressed or outdated features that do not conform to the current upgrade.

3. In the list dialog, select **Repair** to replace any mismatches with the appropriate default.

4. If you receive errors related to customized fields that are important to your operation, see Invoking Setup and built-in error checking (page 39).

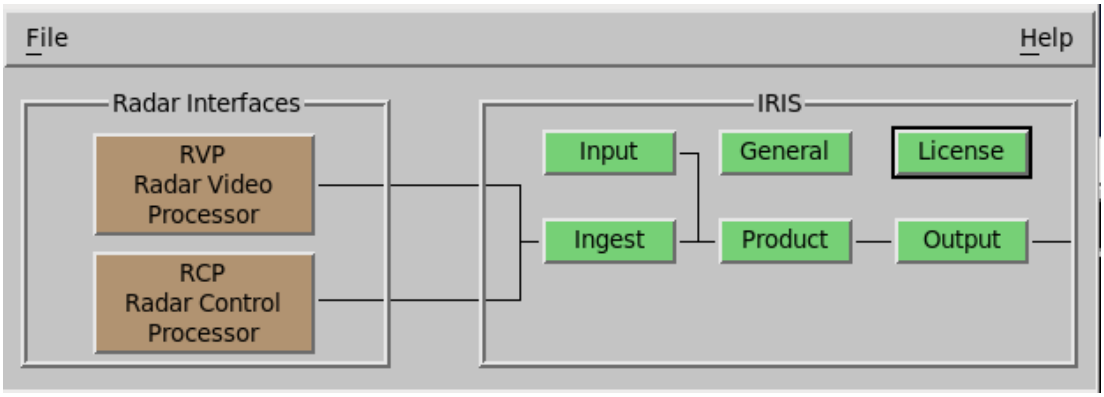
7.4.1 Invoking Setup and built-in error checking

When IRIS starts, it performs configuration and bounds checks.

For new users, the **Setup** parameters are typically correctly set and do not cause any configuration errors. If an error does occur, follow these steps.

1. In the terminal window, type: **`setup&`**

   The **Setup** utility launches.



> There are 2 variants of the **Setup** utility: one for IRIS and one for the RDA (RVP signal processor or an RCP8 antenna controller).
> The RDA variant does not show the IRIS setup features.

2. Select the part of the system setup you want to check or configure.
3. Make your changes and close the window for the selected part of the system.
4. Select **File > Save**.

   The configuration files are now updated.
5. To create a listing file of the **Setup** configuration:
   a. Select **File > List**.

      A listing file called *`YYYYMMDDHHMM.setup`* is created in the *`${IRIS_LISTINGS}`* directory.

6. To take the configuration changes into effect, restart the application:
   a. For changes made to the **Setup > IRIS** section, restart the IRIS daemons by typing:

```
qiris
siris
```

   b. For changes to the **Setup > RVP** section, stop any running utilities with the command `systemctl stop <service unit>`, for example:

```
systemctl stop iris rvp10 rcp8
```

   c. Restart the utilities with the command `systemctl start <service unit>`, for example:

```
systemctl start iris rvp10 rcp8
```

   RVP has a configuration state accessible through **dspx**. Part of that state is local to the processor and part of it is also visible in **Setup > RVP**.

   d. For changes to the **Setup > RCP** section, in addition to the above, you must stop RCP8 (if you have one), and stop the antenna daemons, by typing:

```
$ qiris
$ sudo systemctl stop rvp10
$ sudo systemctl stop rcp8
$ qant
$ sudo systemctl start rcp8
$ sudo systemctl start rvp10
$ siris
```

   RCP8 has a configuration state accessible through **Antx**. These changes take effect when you return to the top level prompt. You must save your changes.



License changes can affect RVP and IRIS.

7. If an error list is displayed,
   a. Check the error list for parameters that you have customized and correct these customizations.
   b. Select **Repair** to make corrections that are necessary for the software but do not need to be customized for your operation.
   c. Select **File > Save**.

7.5 Checking the kernel module status

After installation or upgrade, check that the RDA kernel module has been installed and loaded. If the kernel module has not been loaded, the rvp10 process will not start.

To check this, type:

```
lsmod | grep rda
```

If no data is displayed, the kernel module has not been loaded or installed properly.

To check the status of the kernel module, type:

```
systemctl status systemd-modules-load.service
```

If the kernel module is not running, start the module by typing:

```
systemctl start systemd-modules-load.service
```

8. Configuration

8.1 Configuring passwords

The IRIS RDA default password policy has changed into a stricter one starting at release 10.4. This is due to CIS server hardening and recommendations set by Center for Internet Security (CIS).

8.1.1 Changing password policy

NOTICE! Vaisala strongly recommends using a strict password policy. Taking into use a password policy that is less strict than the one set by Vaisala by default is not recommended.
The default password policy set for IRIS RDA software is based on recommendations by Center for Internet Security.

Password length

Set in file */etc/security/pwquality.conf* or by adding a new configuration file in path: */etc/security/pwquality.conf.d*

Variable: `minlen = 14`

Default: **14**

Password quality

Set in file */etc/security/pwquality.conf* or by adding a new configuration file in path: */etc/security/pwquality.conf.d*

Variable: `minclass = 4`

`-- AND/OR --`

`dcredit = -1` # To force at least 1 digit (Set to for example to -3 to force at least 3 digits to be used)

`ucredit = -1` # To force at least 1 upper case character

`lcredit = -1` # To force at least 1 lower case character

`ocredit = -1` # To force at least 1 other character

Default: characters from 4 classes (minimum)

Password max consecutive characters

Set in file */etc/security/pwquality.conf* or by adding a new configuration file in path: */etc/security/pwquality.conf.d*

Variable: `maxrepeat` = 3

Default: **3**

Password max sequential characters

Set in file */etc/security/pwquality.conf* or by adding a new configuration file in path: */etc/security/pwquality.conf.d*

Variable: `maxsequence = 3`

Default: **3**

Password expiration

Set in file: */etc/login.defs*

Variable: `PASS_MAX_DAYS 365`

Default: **365**

8.2 Configuring RDA software

After the receiving your unit from the factory, or after software re–installation, you must configure the software to customize your system for your environment and application.

Table 5 RDA configuration tools

Configuration tool	RDA device	Description
setup/RVP utility *setup_dsp.conf* See *IRIS and RDA Utilities Guide (M212925EN)*.	RVP10	Configures the local environment required to run RVP support utilities such as **Ascope** and **dspx**. Examples: radar equation parameters that are required for calibration, pulse width definitions, and PRF request limits.
setup/RCP utility *setup_ant.conf* See *RVP10 User Guide (M212604EN)*.	RCP8	Configures the local environment required to run the RCP8 support utilities that such as **Antenna** or **Bitex**. Examples: max allowed AZ/EL velocity request, MIN and MAX elevation angles that can be requested, and LAT/LON of radar for sun tracking.
RVP10 NV setups *rvp10.conf* See *RVP10 User Guide (M212604EN)*.	RVP10	Defines the details of the sampling and processing algorithms, as well as the operational configuration of the system. Examples: IF filter design and selection, PRF limits, relative trigger timing, dual-polarization features.
RCP8 NV setups *rcp8.conf* See *RCP8 User Guide (M212923EN)*.	RCP8	Configures which status and control bits are available and define the antenna servo control parameters. Examples: physical or virtual tachometer selection, shutdown safety criteria and internal antenna simulator on/off.

Configuration tool	RDA device	Description
profile.conf See *RVP10 User Guide (M212604EN)*	RVP10	Configures the network interface from RVP10SRV server to IFDR10.
softplane.conf See *RVP10 User Guide (M212604EN)*	RVP10 RCP8	Defines the I/O signals on the I/O-62 connector panel, pin-by-pin. Examples: whether a line is an input or output, electrical specification such as RS422 or TTL, what local variable name is associated with each line.

During installation, you must configure the **Setup** utility and the TTY setups for your system.

The configuration results are stored as ASCII text *.conf* files, typically in the */etc/vaisala/irisrda* directory. Each file has a factory default configuration file that is stored in the template directory. The default is:

```
/etc/vaisala/irisrda/templates/init/
```

For a radar network with identical hardware, you can perform configuration maintenance by copying pre-tested files over the network.

8.3 Configuring firewall

By default, the firewall is configured to be active in the AlmaLinux installation. However, some modifications are needed to enable communications between units.

By default, the IRIS server firewall is configured so that the NTP service is allowed from the outside network.

NTP service is added to firewall configuration by RVP10 post-install script.

Additionally, WRM200 factory configuration disables firewall on IFDR10 and radar cabinet network interfaces. WRS300 and WRS400 factory configuration disables the firewall on radar cabinet network (IFDR is in the same network).

8.3.1 Configuring the firewall

IRIS Focus connects to IRIS Analysis using port 30735. By default, the firewall of the IRIS Analysis server blocks this port. When IRIS Analysis and IRIS Focus are installed on separate servers, you need to configure IRIS Analysis server to allow the connection to this port:

1. Log in to the IRIS Analysis server as **admin**.
2. Run the following commands:

```
sudo firewall-cmd --add-port=30735/tcp --permanent
sudo firewall-cmd -reload
```

8.3.2 Configuring the IFDR10 interface

On the interface to IFDR10, the firewall should be disabled. To do this, move the interface to the trusted zone. IFDR10 also needs the `ntp` service. It can be added to the allowed services.

1. Use the following commands:

```
sudo firewall-cmd --zone=trusted --change-interface="rvp10_interface" --
permanent
sudo firewall-cmd --add-service=ntp --permanent
sudo firewall-cmd --reload
```

In the command, replace `rvp10_interface` with the real interface name.
You can find the interface name by looking for the network interfaces in radar server. In the following example, we know that RVP10 is connected to 10.0.3.x network, and from the listing below we see that the name for that interface is **ens6f1**.

```
$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
.....
4: ens6f0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state
DOWN group default qlen 1000
    link/ether 04:42:1a:1d:7d:3a brd ff:ff:ff:ff:ff:ff
    altname enp59s0f0
5: ens6f1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
group default qlen 1000
    link/ether 04:42:1a:1d:7d:3c brd ff:ff:ff:ff:ff:ff
    altname enp59s0f1
    inet 10.0.3.1/24 brd 10.0.3.255 scope global noprefixroute ens6f1
       valid_lft forever preferred_lft forever
```

8.3.3 Radar cabinet interface

Typically, the radar cabinet network interface can be moved to the trusted zone. Use the following command and replace `radar_cabinet_interface` with the real interface name. To find the interface name, look for the network name of the radar cabinet network (typically, 10.01.x and 10.0.2.x networks).

```
sudo firewall-cmd --zone=trusted --change-interface="radar_cabinet_interface"
--permanent
sudo firewall-cmd --reload
```

8.3.4 Remote IRIS menu interface

To be able to connect to the radar server IRIS from the remote IRIS menu, the firewall must be configured to allow all traffic from selected IP addresses. In the following command, replace `<IP_ADDRESS>` with the real IP address of the IRIS machine connecting to radar.

```
sudo firewall-cmd --zone=trusted --add-source=<IP_ADDRESS> --permanent
sudo firewall-cmd --reload
```

VNC connections to radar server

If you want to use a VNC connection to the radar server, you need to allow the `vnc-server` and selected ports through the firewall. You can check the services using the following command:

```
$ sudo firewall-cmd --list-services
cockpit dhcpv6-client ntp ssh vnc-server
```

Add allowed services using the following commands:

```
$ sudo firewall-cmd --add-service vnc-server --permanent
$ sudo firewall-cmd --reload
```

Additionally, you must open the ports used by VNC. As an example, if `TigerVNC` server is started in port 5, you need to open port 5905. The default port for `TigerVNC` is 5900, and when an additional port N is configured, the firewall port 5900+N must be opened. In the example, a range of ports is opened, too.

```
$ sudo firewall-cmd --add-port=5905/tcp --permanent
$ sudo firewall-cmd --add-port=5910-5920/tcp --permanent
$ sudo firewall-cmd --reload
```

Allowed ports can be checked by the following command:

```
$ sudo firewall-cmd --list-ports
```

8.4 Configuring SSH

You must set up an ssh connection from one computer (the **host**) to another (**target**) so that users can login from **host** to **target** without a password, and IRIS can send data from the **host** to the **target**.

1. Log in to the host computer as **admin**.
2. Check if *.ssh* directory exists.

   If not, then create the directory by typing:

   ```
   sudo ssh-keygen -t rsa
   ```

   When prompted with questions, press **Enter** without typing anything.
3. Type:

   ```
   sudo ssh-copy-id -i id_rsa.pub radarop@remotehost
   ```

4. When prompted for login, enter the **radarop** password.
5. After a successful login, log out again.
6. On the host computer, test the SSH connection as **admin** with the command:

   ```
   sudo ssh radarop@remotehost date
   ```

   You should get the date and time display from the remote host without a password prompt.

You can now send data from the **host** computer to the **target** through the IRIS product output menu.

9. Installing IO-62 firmware

If you have installed or upgraded the RDA software, and your system includes an IO-62 card and connector panel, you must update the firmware running on RCP8 to be compatible with the installed RDA software.

1. Login as **admin**.
2. Check for running processes by typing:

```
sudo ps-iris
```

3. Stop any running processes by typing:

```
sudo qiris
sudo quant
```

4. Log in as **radarop** (default password **Vaisala!factory**).

   You enter X–Windows.
5. Right-click and start a terminal window.
6. For each Vaisala component, type the appropriate command. For example:

Vaisala component	Command
Standard I/O-62 card	`io62-0`
Standard connector panel	`io62cp-0`

7. Shut down the system by typing:

```
poweroff
```

8. When **Power down** is displayed, turn power off with power switch on lower right of front panel.

   The FPGA software installation is complete.
9. Reboot the unit.

   Follow the progress of the reboot on the monitor. The front panel LED display shows the time of the reboot and display diagnostic messages.
   The reboot takes about 1 minute.

10. Stop the RCP process by typing:

```
$ killall rcp8
```

11. Run the following diagnostics and observe the results:

```
$ rdadiags io62-0
 $ rdadiags io62cp-0
```

12. Restart the RCP8 process by typing:

```
rcp8 &
```

13. Verify that the restart messages show no faults.
14. Configure RCP.
    See *RCP8 User Guide (M212923EN)*.

10. Installing RVP10 (RDA) firmware

Before installing RVP10 (RDA) firmware, make sure that:

- The second Ethernet port has been configured. See Configuring the system and network (page 72).
- IFDR10 is physically connected to the port.

If you have installed or upgraded the RDA software, you must update the firmware running on IFDR10 to be compatible with the installed RDA software.

1. Reboot the computer.
2. Login as **radarop**.

   The default password is: **`Va1sala!factory`**
   (Note that the first character is capital letter '**`V`**', and the third character is number one '**`1`**'.)
3. If IRIS / RDA services are running, turn them off.
   a. Check what is running.

   ```
   # ps_iris
   ```

   b. If any services are running, stop them.

   ```
   # systemctl stop iris
    # systemctl stop rvp10
    # systemctl stop rcp8
    # systemctl stop dspexport
    # systemctl stop antennad
   ```

4. Verify that all services have stopped:

   ```
   # ps_iris
   ```

   If there are services running, stop them using the **`systemctl`** commands or manually kill them.
   You must be logged in as **`root`** to use the **`kill`** command:

   ```
   # su
    # kill <process ID number>
   ```

5. If not powered, power on IFDR10, and wait for it to boot.
6. If the network cable is not attached, attach IFDR10 to the second Ethernet connection configured for the 10.0.3.x network.
7. Verify that IFDR10 is accessible over Ethernet.

   Run **`ping`** letting at least 4 packets transmit, and press **Ctrl+C** to exit program. Verify that there is 0% packet loss.

   ```
   # ping 10.0.3.254
   ```

   `10.0.3.254` is the default IP address of IFDR10.
8. Change to the repository where the image is installed (be default */usr/bin*):

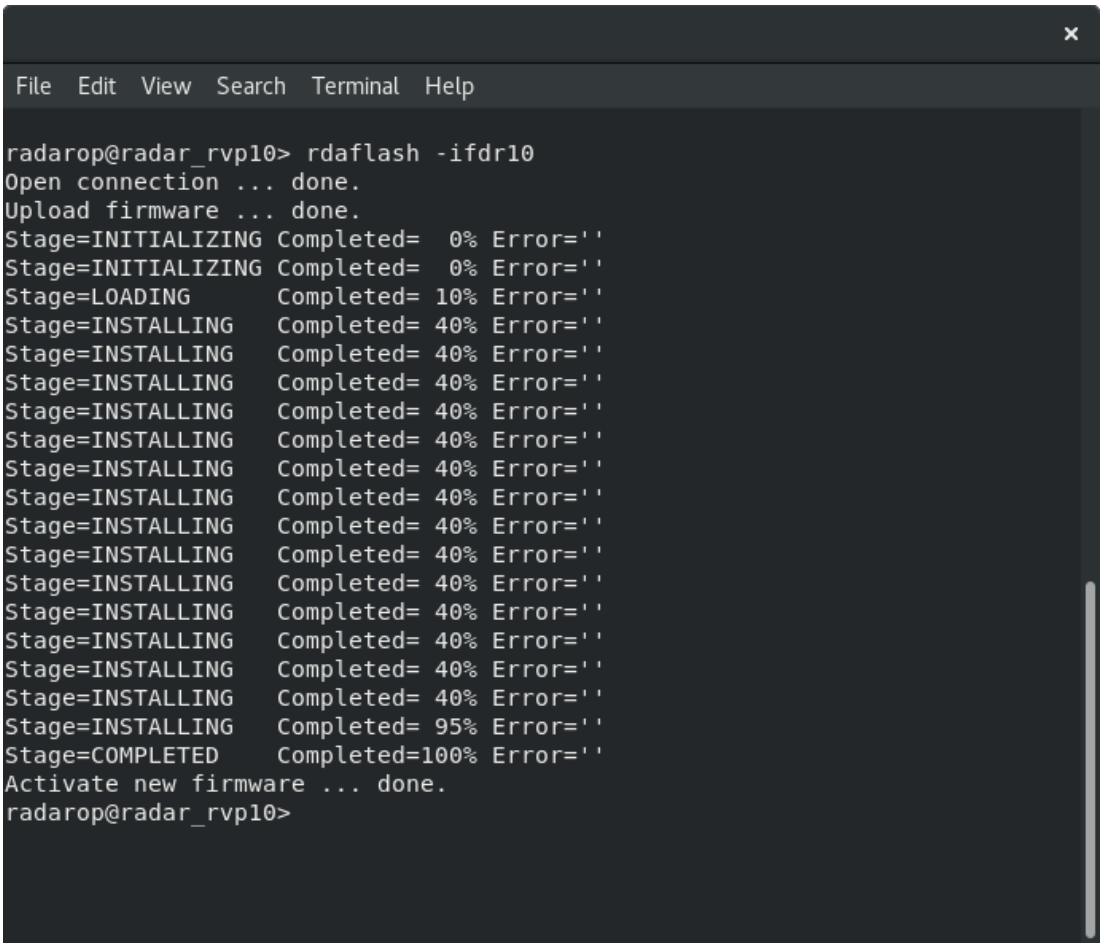
   ```
   cd /usr/bin
   ```

9. Use the **rdaflash** utility to update the IFDR10 firmware:

```
rdaflash -ifdr10
```

This takes several minutes. Do not interrupt programming.

NOTICE! When programming starts, do not power cycle or reboot IFDR10 until `rdaflash` is successfully completed.



When the programming is complete, IFDR10 reboots.

10. Reboot the computer and login as **radarop**.
11. Verify that the expected process are running with the command:

```
# ps_iris
```

12. Configure RVP.

    See *RVP10 User Guide (M212604EN)*.

13. If the upgrade is interrupted or not completed successfully, the unit stays in diagnostic mode on the next reboot so you can recover from the failure.
14. For RVP upgrades, if the RDA software boots, but is unresponsive, you can force the RVP into diagnostic mode by sticking a paper clip in the inner most hole on the side of the enclosure.

    After entering the diagnostic boot mode, you can re-flash the IFDR10 software from the signal processor to recover from a corrupted image.

If the IFDR10 firmware upgrade is part of a software upgrade process, see Running Setup after upgrade (page 39).

11. Login, logout, and shutdown

11.1 Powering up

When you power-up the computer, the system goes through an automatic startup of the operating system at the end of which the software starts and performs power–up self tests.

If you are not doing any diagnostic or software maintenance work on the system, there is no need to log-in after power-up. When you turn the unit on, your application software takes over.

11.2 Local and remote login

You can login either locally or remotely.

- Login locally using the local workstation or through a KVM.
- You can login remotely if `ssh` is enabled. Check with your network administrator.

Here, we assume a local login is used.

11.3 Default usernames and passwords

The standard software installation defines the following standard users:

- `radarop`
- `observer`
- `admin`

For servers installed at Vaisala, the default password is: `Va1sala!factory`

(Note that the first character is capital letter '**V**', and the third character is number one '**1**'.)

> **NOTICE!** For security reasons, changing the password is strongly recommended.
> For password rules, see Password policy (page 9).

To run commands that require **root** privileges, log in as **admin**, and type `sudo` at the beginning of the command.

The system administrator can change passwords using the standard Linux password support.

11.4 Running commands with root privileges

IRIS RDA software does not include a **root** account. To run commands that require **root** privileges:

1. Log in as **admin**.

   For servers installed at Vaisala, the default password is: **`Va1sala!factory`**

2. Type **`sudo`** at the beginning of the command.

11.5 Local login as operator after powerup

1. At the power-up login prompt, type **`radarop`** and press **Enter**.

   When prompted, provide the password (default password is **`Va1sala!factory`**). An X-Window screen appears.

2. Right-click and select **New Window** to get a terminal window.

   The top of the terminal window shows your user name, the node name of the system, and the current directory path.

11.6 Powering off

1. Type **`poweroff`**.

   The system goes through a shutdown sequence. When it is done, **Power down** is displayed.

12. Troubleshooting

12.1 Correcting file ownership and protection

Sometimes, when starting a program or trying to access calibration files, users cannot access some files or they receive an error message saying they do not have privileges to do an operation.

This is because the file ownership and protection settings are incorrect.



Do not change the file protection manually. Always use the **`sigmet_env -setown`** command to fix the protection of your files.

1. To correct the file ownership and protection, type:

   ```
   # sigmet_env -setown
   ```

   The script goes through the */etc/vaisala* directory tree, changing the ownership of the files to **`operator`** and setting the protection as follows:
   - Directories—**`rwxrwxr-x`**
   - All files, except executable files—**`rwrw-r--`**
   - Executable files—**`rwsrwsr-x`**

12.2 Authorizing remote X–Windows on your node

1. To enable IRIS systems running on other nodes to send output to your screen, enter the command:

   ```
   $ xhost  +<host>
   ```

   Where **`<host>`** is the remote hostname, or IP address.
2. Check that this works as you intend.
3. Add the appropriate command at the end of one of the following files:
   - To authorize the windows as soon an anyone logs in: */etc/profile.d/sigmet.sh*
   - To support just one user authorizing the windows: home directory *.bash_profile*

12.3 Making Quick Look Windows (QLW) appear

For any problem that prevents the window from starting, IRIS prints:

```
OUTPUT, Error in open_display call.
```

The **Radar Status** menu also indicates **Error** and **Exit** next to the window process.

If you cannot identify the problem from the error message:

1. Check that the workstation is turned on and the network is up and running.
2. Login as **`radarop`**.
3. Open the **Radar Status** menu and toggle the **Product Output** process off/on.
4. In the command prompt of the workstation where the window should appear, check the user rights by typing:

   ```
   xhost+
   ```

5. Restart IRIS on your workstation by typing:

   ```
   sudo systemctl restart iris
   ```

   NOTICE! This command restarts all IRIS processes.

   IRIS tests each process and restarts any that have stopped.

6. If the IRIS Quick Look Window (QLW) does not appear after typing **`siris`** in a terminal window:
   a. Log in as **`root`**.
   b. In the first line of the */etc/hosts* file, add the host name to the first line of the file:

   ```
   127.0.0.1 <host-name> local host...
   ```

7. If the steps above do not help, make sure the **Display name** is correct:
   a. In the terminal window, check the value of `DISPLAY` with the command:

      ```
      echo $DISPLAY
      ```

      Typical values for local DISPLAY are `:0` and `:1`.
   b. Open the **Setup** utility.
   c. In the **Output Device Setups** section, type the `DISPLAY` value into the **Display name** field.

      Check if the QLW now appears.

12.4 Replacing failed OS RAID disks

RAID1 is automatically configured on the server. However, in some cases, you may need to remove, recover, and add new devices to RAID.

In most cases, this requires removing the failing disk and installing a new one.



While you can do this while powered up, if the system allows you to power down, do so.

1. To check the status of the RAID1 disk, type:

   ```
   cat /proc/mdstat
   ```

   When RAID1 is working correctly, the terminal prints, for example:

   ```
   Personalities : [raid1]

   md126 : active raid1 sda[1] sdb[0]

         125032448 blocks super external:/md127/0 [2/2] [UU]

   md127 : inactive sdb[1](S) sda[0](S)

         4520 blocks super external:imsm
   ```

   - `[UU]` indicates that both disks are operational.
   - If there is a problem with one of the disks, the `[UU]` string is `[_U]` or `[U_]`.
2. Check if disk `sda` or `sdb` has failed.

3. To remove the disk from RAID configuration, type:



Take care when removing the failing disk.
Remove only the disk identified as failing. In the following example, it is **sdb**.

```
mdadm --manage /dev/md/imsm0 --remove /dev/sdb
```

The terminal prints:

```
mdadm: hot removed /dev/sdb from /dev/md/imsm0
```

4. Power down computer, replace the failing disk, and reboot
5. To create the partition on the replacement disk, type:

```
sfdisk -d /dev/sda | sfdisk /dev/sdb
```

6. To verify the partition, type:

```
fdisk -l
```

7. To add a new disk to the raid array, type:

```
mdadm --manage /dev/md/imsm0 --add /dev/sdb
```

8. To check the recovery process, type:

```
cat /proc/mdstat
```

The terminal prints:

```
[root@wes-install ~]# cat /proc/mdstat

Personalities : [raid1]

md126 : active raid1 sdb[2] sda[1]

      125032448 blocks super external:/md127/0 [2/2] [UU]

md127 : inactive sdb[1](S) sda[0](S)

      4520 blocks super external:imsm

 unused devices: <none>
```

Appendix A. Installing AlmaLinux

A.1 Overview to installing AlmaLinux



This version of IRIS RDA can be run on the AlmaLinux 9 or AlmaLinux 10 operating system.

Vaisala provides customized ISO images for AlmaLinux 9.7 and AlmaLinux 10.1 on the Vaisala FTP website:

https://ftp.sigmet.vaisala.com/files/releases/AlmaLinux/

Vaisala supports two installation methods from the Vaisala spin version of the ISO image:

- Automatic - unattended installation
- Manual - interactive installation

For both installation methods you can use the local USB device as your installation media.

We recommend that you use the automatic process unless you have special system configuration needs or if your custom configuration fails the automatic installation process.

Installing Linux requires a Linux software installation tree and a boot device. You must transfer the AlmaLinux distributions ISO images to the media that you are going to use in the installation.

You need the following to create installation media:

- PC running Windows 10/11, or AlmaLinux
- USB port and USB Flash Drive 64 GB
  Vaisala recommends a USB 3.0 drive because data transfer is much faster than USB 2.0.

A.2 Creating installation media

Start the installation process by creating and initializing the installation media.

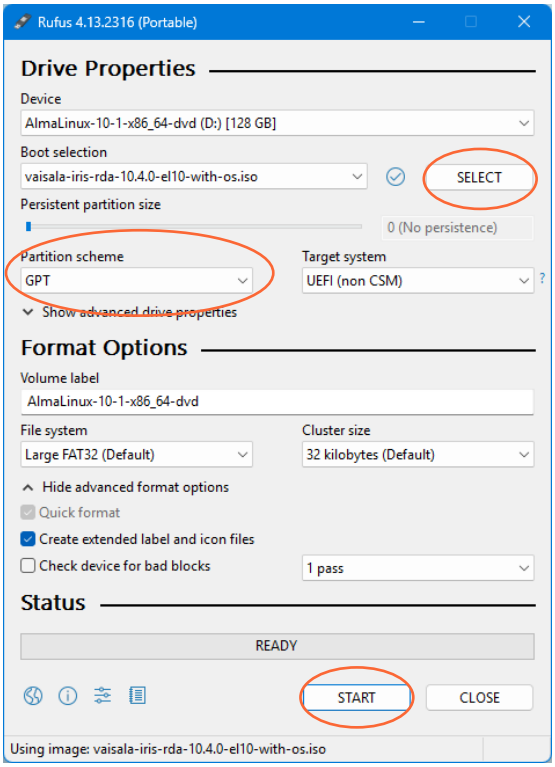
A.2.1 Creating USB installation media on Windows

These instructions apply to Windows 10 and Windows 11.

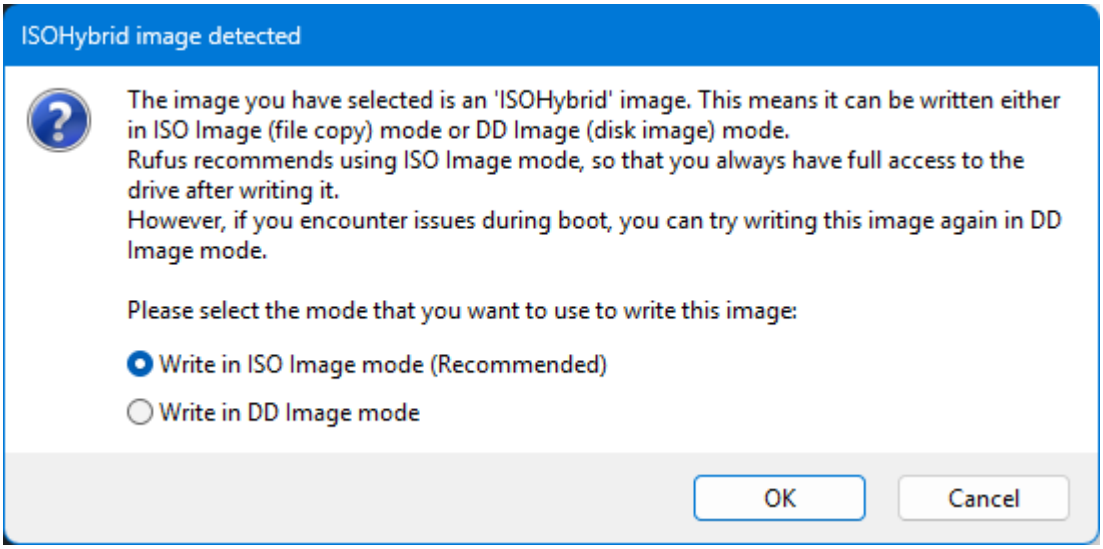
When creating USB installation media on Windows, use a standalone program such as **Rufus** (available at http://rufus.akeo.ie/). Follow the on-screen instructions.

1. Launch **Rufus** by double-clicking the program icon.
2. Insert a USB drive in the USB port.
3. In the **Rufus** window, click **Select**, and select the iso image.

4. In the **Partitition scheme** drop-down menu, select **GPT**.
5. Select **START**.



6. When the **ISOHybrid image detected** pop-up window opens, select **Write in ISO Image mode**.
7. Select **OK**.



8. If the program asks for a permission to find a `grub2` bootloader online, reply `Yes`.

9. When the USB media is ready, select **Close**.

A.2.2 Creating USB installation media on Linux (AlmaLinux)

> **NOTICE!** This operation destroys data on the device you operate on.

1. Run **`$ lsblk`** to list block devices on your system. Take note of the output.
2. Insert a USB drive in the USB port.
3. Run **`$ lsblk`**.

   Compare the output to the previous step. The additional block device from this output is your USB drive.
4. Run **`$ dd if=path/toAlmalinux.iso of=/dev/xxx`**

   Where */dev/xxx* is the path to the USB drive. Do not use the partition number for the USB drive.
   For example: */dev/sdc*.

A.3 Installing AlmaLinux automatically

The automated installation uses KICKSTART to run an unattended installation.

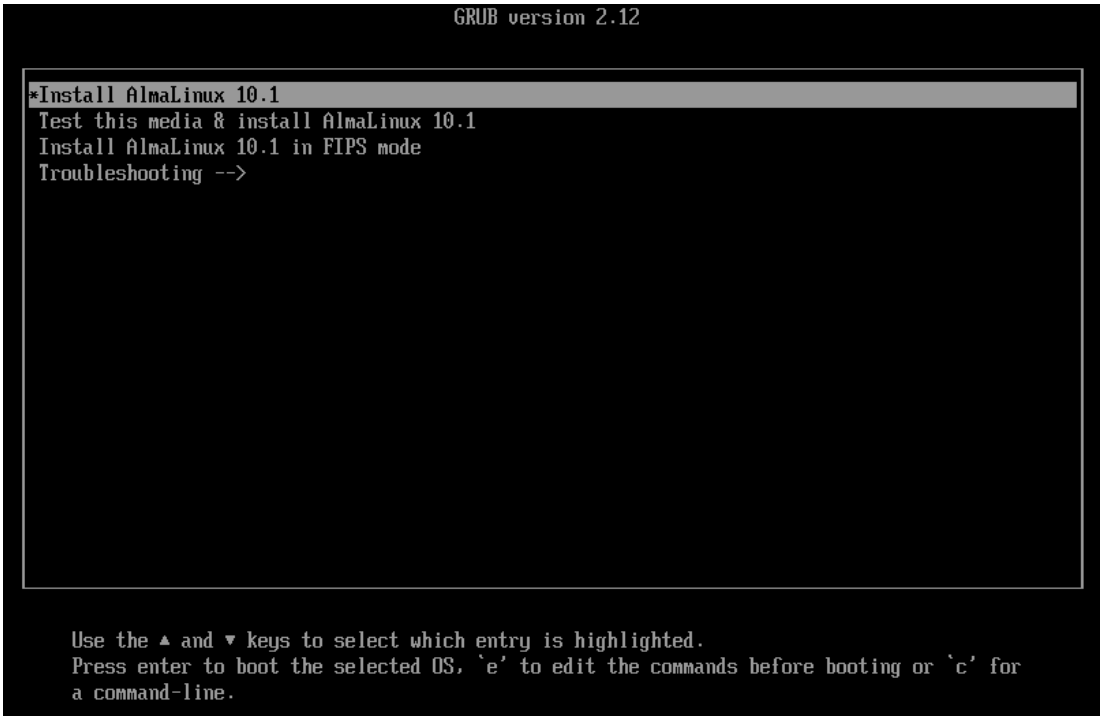
The instructions in this section are for the Vaisala-provided server. If you are using a different system, consult your systems manual for instructions.

1. Power up the system by pressing the power button on the server.
2. Insert the USB drive into the USB port. If you are using the USB port for the first time, this also enables the port.

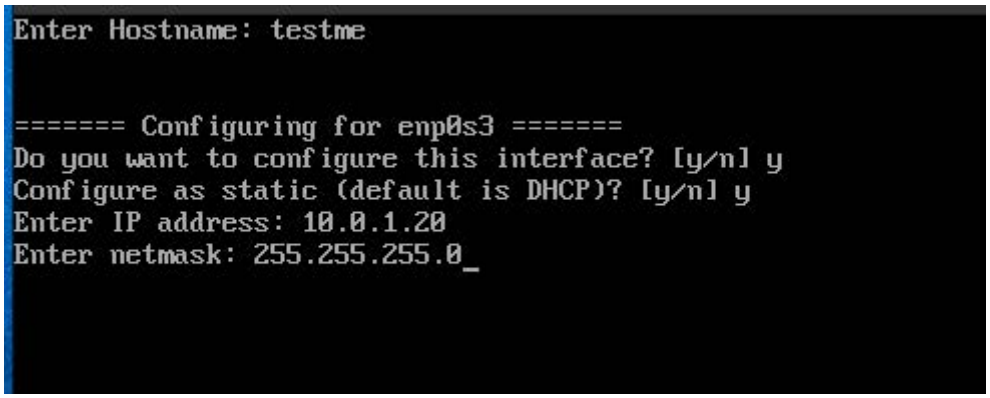
3. In the AlmaLinux window, select the option **Install AlmaLinux**, and press **Enter**.



Do NOT select the option **Test this media and install AlmaLinux**.



4. The installation starts. When prompted, configure the hostname and IP address.
   - For one port, configure the internal network: Select **Configure as static (default is DHCP)?**: `Y`, and enter the IP address `10.0.2.1`.
   - Configure a second port as DHCP by selecting **Configure as static (default is DHCP)?**: `N`.



   Then the installation will continue.

   a. In the **Installation Summary** window, select **Installation Destination**.
   b. Create new partitions: `/`, `/boot`, `swap`, `/srv`, and `boot/efi`.

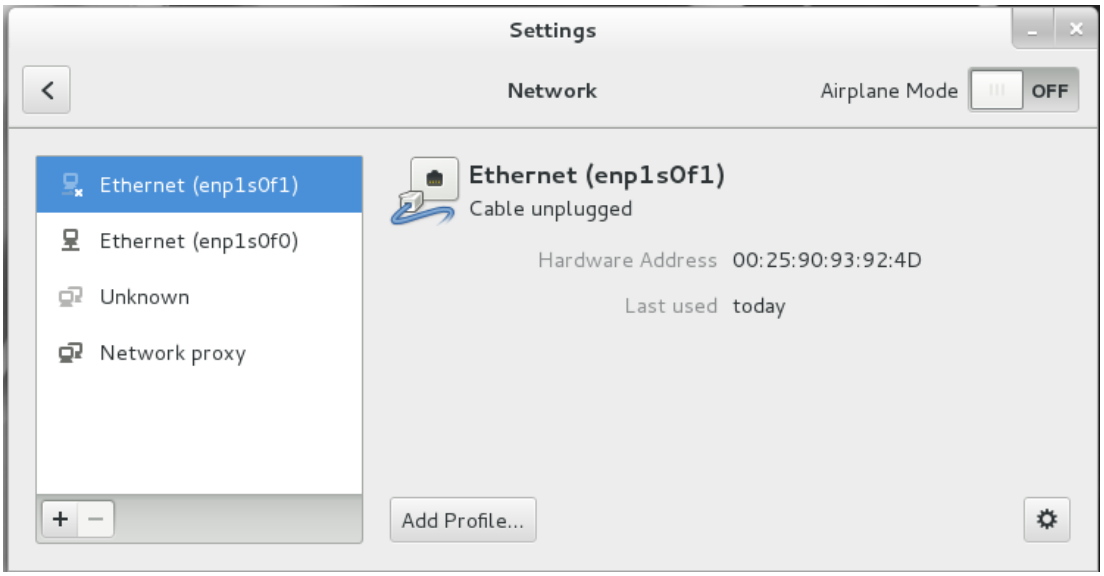
      See chapters Partitioning the destination disk (page 77) and Recommended partitioning settings (page 77).
   c. In the **Installation Summary** window, select **Begin Installation**.
5. When the installation is complete, the system will reboot automatically.
6. Vaisala strongly recommends changing any default passwords.
7. Select **Application > System Tools > Settings GUI**.
8. In **Region & Language**, configure your language settings.

9. Depending on your configuration, you may need to configure the ports.
   - If you are using `Dell PowerEdge R440` server, use ports **em1** and **em2**.
   - If you have an `American Megatrend` server, your `enp9s0` port is automatically set to communicate with the IFDR10 on a 10.0.1.x network.

> **NOTICE!** Do not reconfigure the network port to IFDR10.

   - If you have a `SuperMicro` server, your network settings for IFDR10 are not pre-initialized. The IFDR10 10.0.1.x network is usually configured on the `enp9s0`, `enp1s0f1`, or `eth1` ports but is not limited to these ports.
     This example uses the `enp1s0f1` port.

Select **System Tools > Settings > Network**.



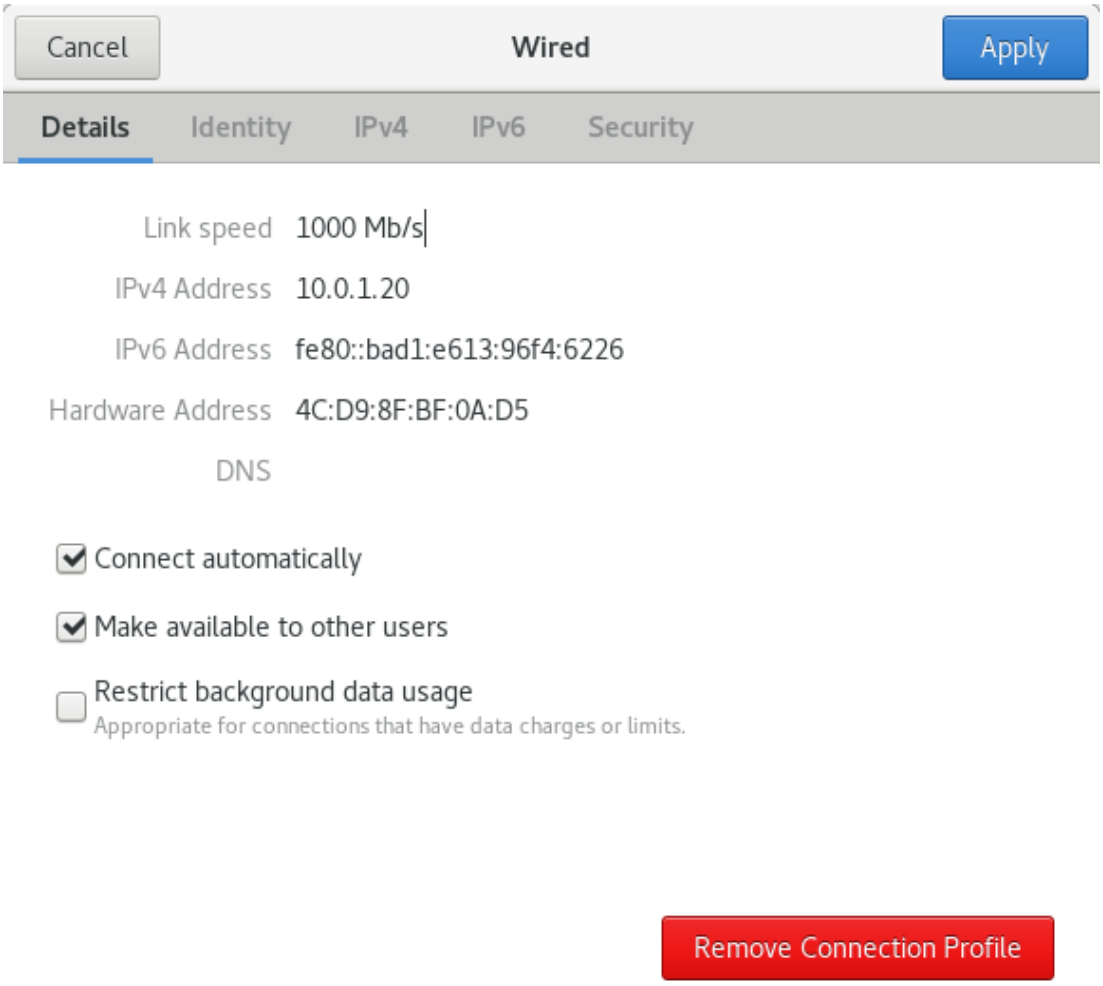
10. In the **Network** window, select the gear icon in the lower right corner.
    In **MTU**, type `8192`.



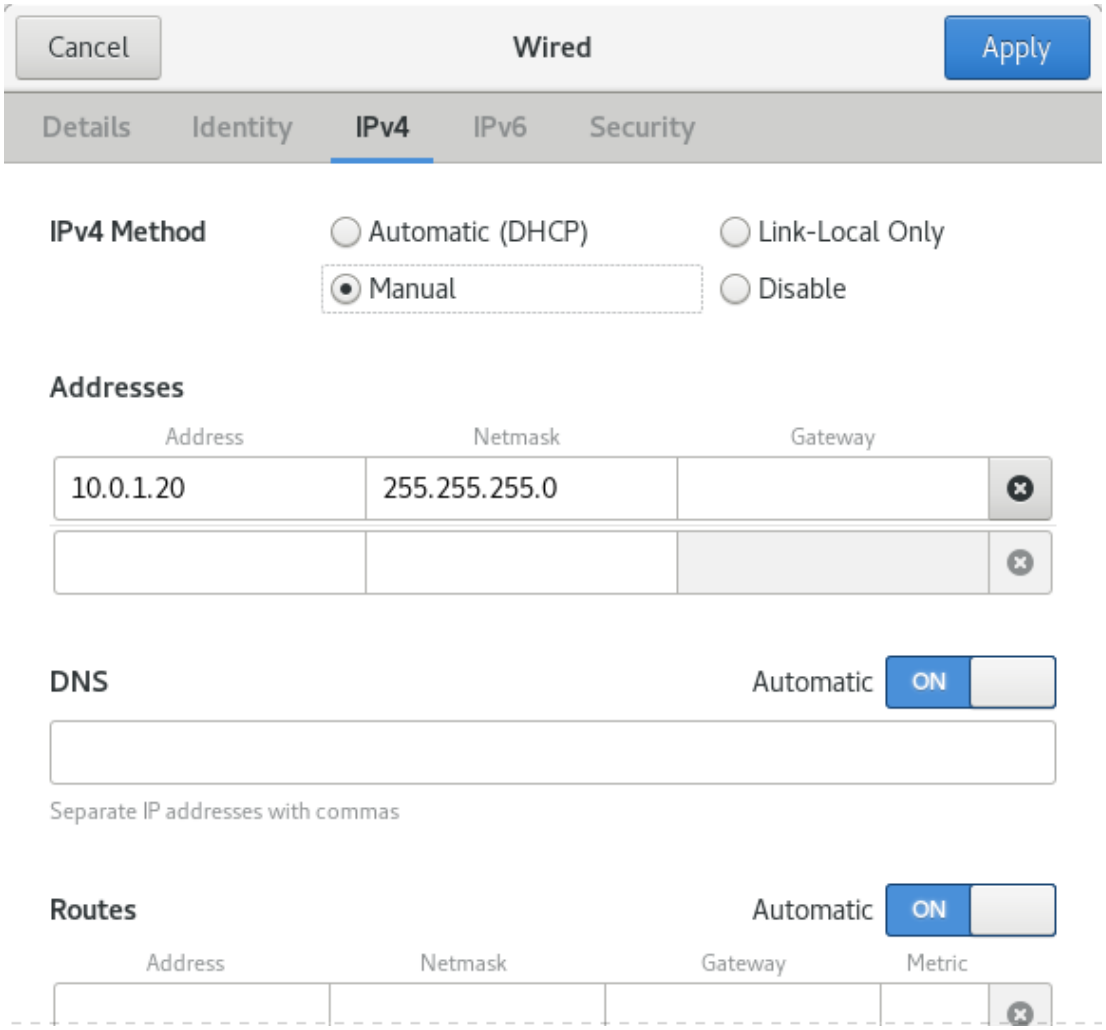
11. Select the **Identity** tab.

12. Select the **Details** tab.

    Select **Connect automatically** and **Make available to other users**.



13. In the right pane, select **IPv4**.



Change **Addressing** to **Manual**.
In the **Address**, **Netmask**, and **Gateway** fields, type enter the test shown in the figure.
Select **Apply**.

More information

- Recommended partitioning settings (page 77)

A.4 Installing AlmaLinux manually (interactive)

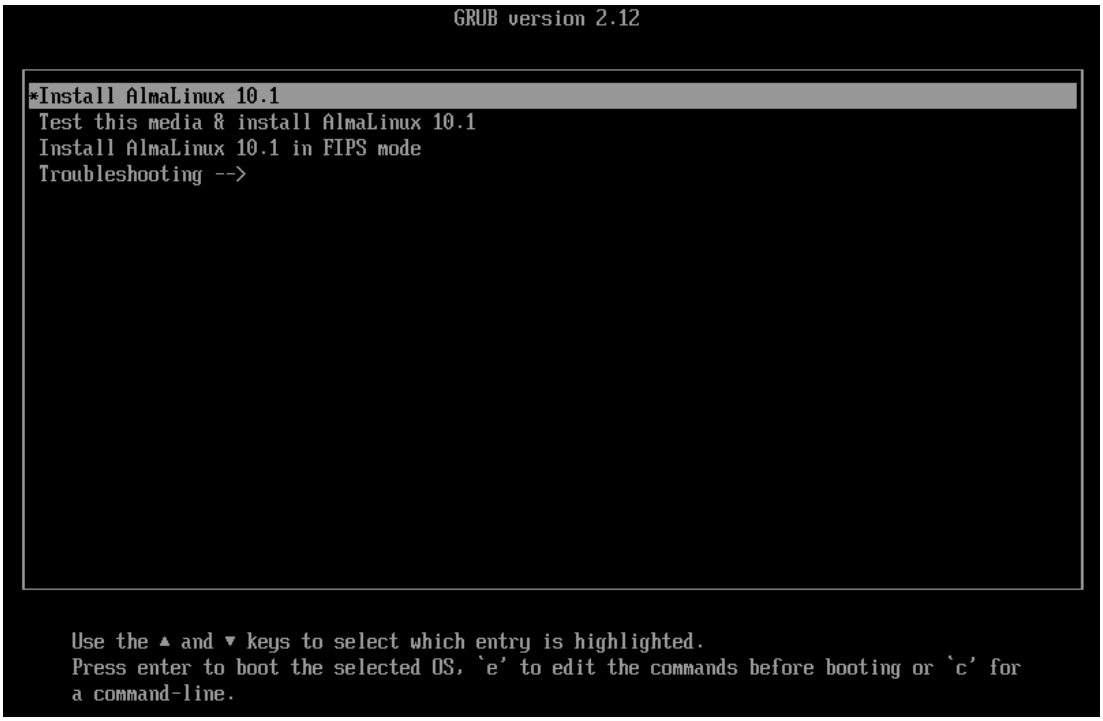
A.4.1 Booting the system for manual installation

You must configure the system to boot from the media device that you have created.

The instructions in this section are for the Vaisala-provided server. If you are using a different system, consult your systems manual for instructions.

1. Power up the system by pressing the power button on the server.
2. Insert the USB drive into the USB port. If you are using the USB port for the first time, this also enables the port.
3. In the AlmaLinux window, select **Install AlmaLinux**, and press **Enter**.

   Do NOT select the option **Test this media and install AlmaLinux**.



4. Select a language.

   (This instruction assumes that **English (United States)** is selected.)
5. Select **Continue**.
6. Select the keyboard icon to select the keyboard type (default is **English**).
7. Select **Language Support** to select the language.
8. Select **Time & Date** to set up the time and date.
   - Region: **Etc**
   - City: **Coordinated Universal Time**

9. Select **USER CREATION**.

   The **User creation** window opens.

   a. In the user name text box, enter user account name or if you wish to have the user account name generated from the full name, enter the user's full name in the **Full name** text box.

   b. In the password text box, enter the user account's password.

   c. In the confirm text box, re-enter the user account's password.

   d. Select **Done**.

      If your password is weak, you are prompted to select **Done** a second time.

10. For **Installation Source**, select the default value (**Local media**).
11. Select **Software Selection (Server with GUI)**, and for additional software, select **Development Tools**.
12. Click on **Installation Destination**
13. Select local Standard Disks, and check the **Custom** button.
14. Select **Done**.
15. Select **LVM** for the partition scheme from the drop-down menu.

    Select the **+** icon to add a partition. For more information about the partitioning, see Partitioning the destination disk (page 77).

A.4.2 Configuring the system and network

1. In the **Installation summary** window, select **Network & Host Name**.
2. Enter the host name in the **Host name** text box in the lower left corner.

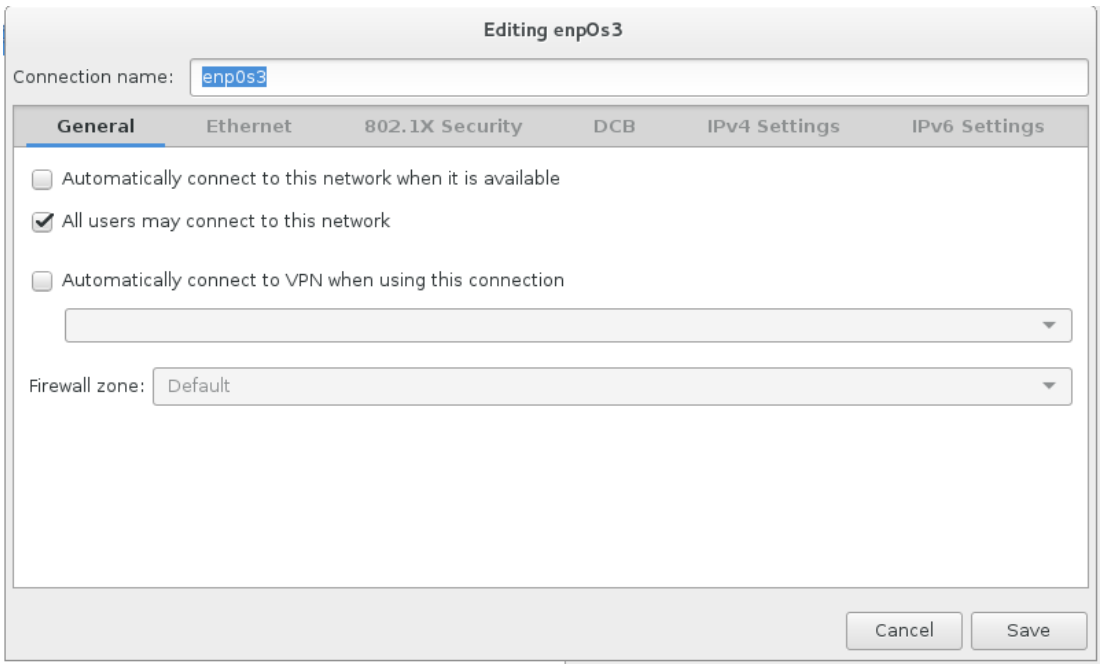
   a. Select the network device you wish to configure listed in the panel on the left hand side. The selected device is highlighted.

   b. In some interfaces, to enable the network interface, select the blank button next to **OFF** in the upper right-hand corner.

      If the button exists, slide the button to the **ON** position.

   c. Select **Configure** at the bottom right-hand corner to display the **Editing** window.

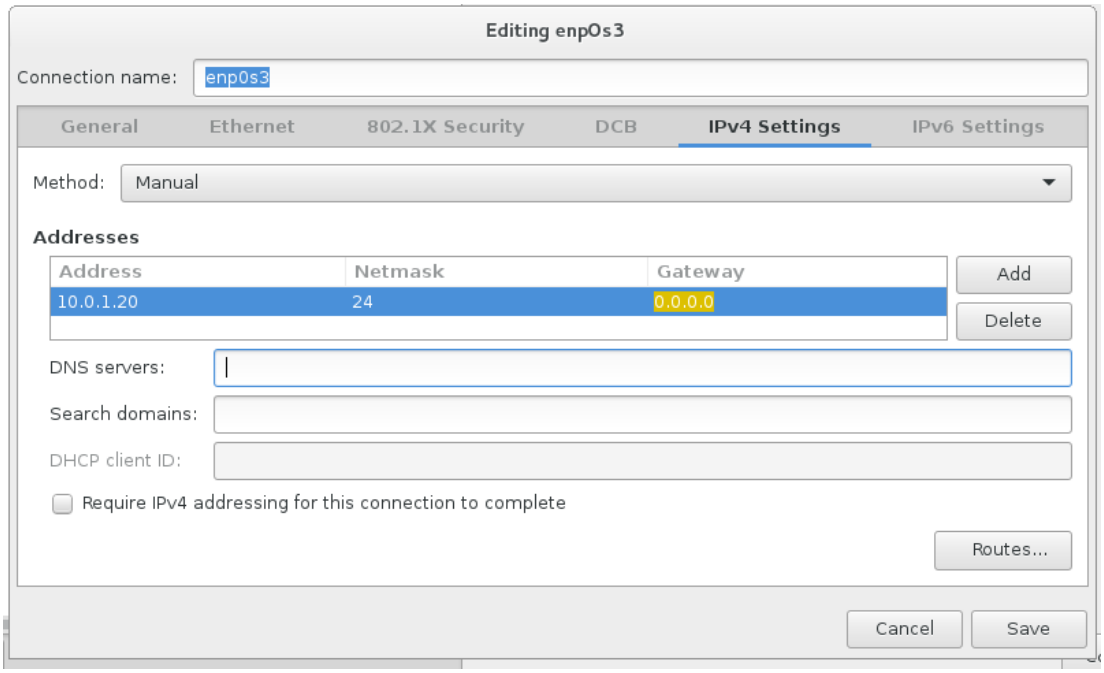
3. Select the **General** tab to set the connectivity options.



a. Select **Automatically connect to this network when it is available**.

b. Select **All users may connect to this network**.

4. Select the **IPv4 Settings** tab.



   a. In the **Method** drop-down menu, select **Manual**.
   b. Select **Add**.
   c. Enter the IP address, netmask, and gateway in the text entry boxes under the headers.
   d. If configuring your `eth0` interface, type your DNS server address in the **DNS server** field.

      If configuring your `eth1` interface, leave this blank.
   e. If configuring your `eth0` interface, type your domain name in the **Search** domains field.

      If configuring your `eth1` interface, leave this blank.
   f. Check the **Require IPv4 addressing for this connection** box near the bottom of the page.
5. Optional: If you are configuring the computer to run RDA software and connect to IFDR10, you need to configure Ethernet ports. See Configuring the system and network for RDA and IFDR10 (page 74).
6. Select **Save** in the lower right corner to finish network configuration.
7. Select **Done** in the upper left corner of the **Network and Host Name** tab to return to the **Installation summary** window.

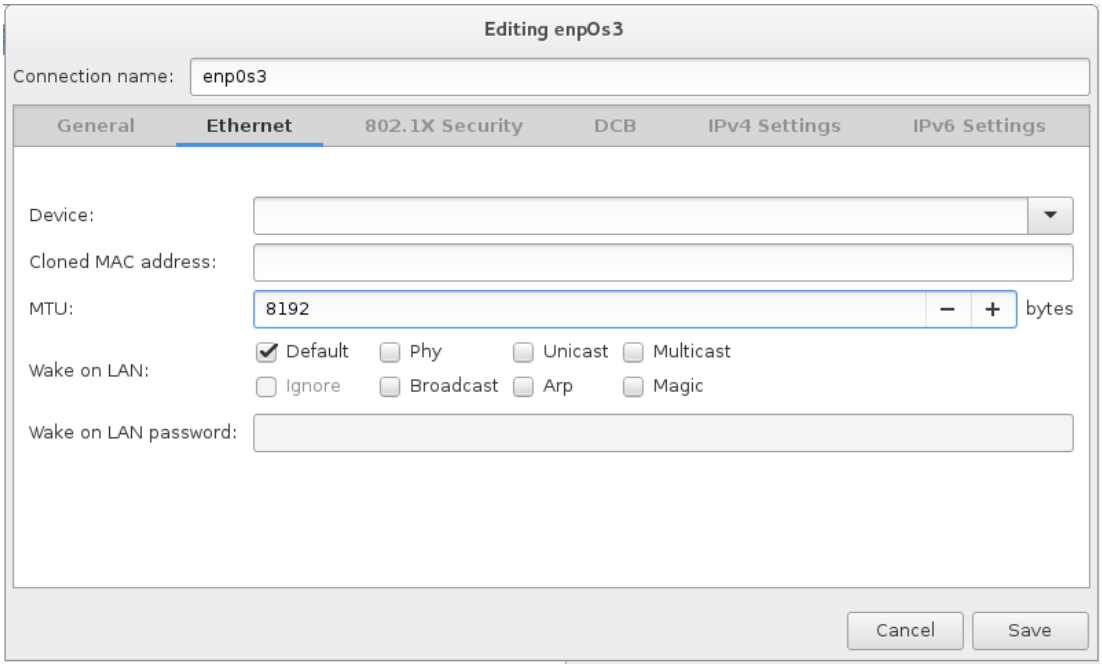
A.4.2.1 Configuring the system and network for RDA and IFDR10

If you plan to run RDA software on this computer and connect to IFDR10, two Ethernet ports are required.

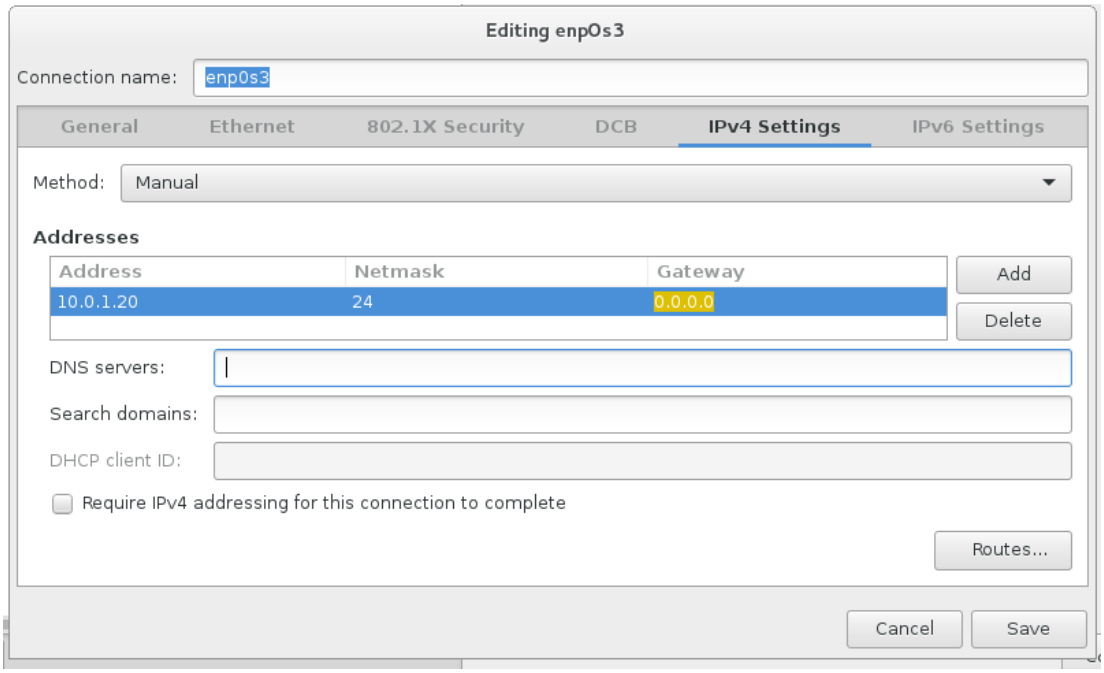
1. In the installation summary page, select **Network and Host Name**.

   The required Ethernet ports should appear in the panel on the left hand side of the **Network and Host Name** window.

2. Select the **Ethernet** tab. In the **MTU** field, type `8192`.



3. Select the **IPv4 Settings** tab.



   a. In the **Method** drop-down menu, select **Manual**.
   b. Select **Add**.
   c. Enter the IP address, netmask, and gateway in the text entry boxes under the headers.
      - If you are configuring the Ethernet port connected to the Internet or your corporate network: The settings in this window are specific to your network configuration. If you are unsure what to enter in these fields, contact your IT support.
      - If you are configuring the Ethernet interface for direct connection to the IFDR10, use the following settings:

Setting	Value
Address	10.0.3.1
Netmask	24
Gateway	0.0.0.0

   d. Type your DNS server address in the **DNS server** field.
   e. Type your domain name in the **Search** domains field.
   f. Check the **Require IPv4 addressing for this connection** box near the bottom of the page.

4. Select **Save** in the lower right corner to finish network configuration.

5. Select **Done** in the upper left corner of the **Network and Host Name** window to return to the installation summary page.

A.4.3 Partitioning the destination disk

A.4.3.1 Recommended partitioning settings

Vaisala recommends the following disk partitioning.

You need the */boot/efi* partition if your computer uses the UEFI boot.

Table 6 Recommended disk partitioning

Partition	File system type	Size
/home	XFS	50 GB
/boot	EXT4	1024 MB
/boot/efi	EFI	600 MB
/var	XFS	100 GB
/	XFS	50 GB
swap	SWAP	size of RAM + 2 GB
/srv	XFS	All of the remaining disk space

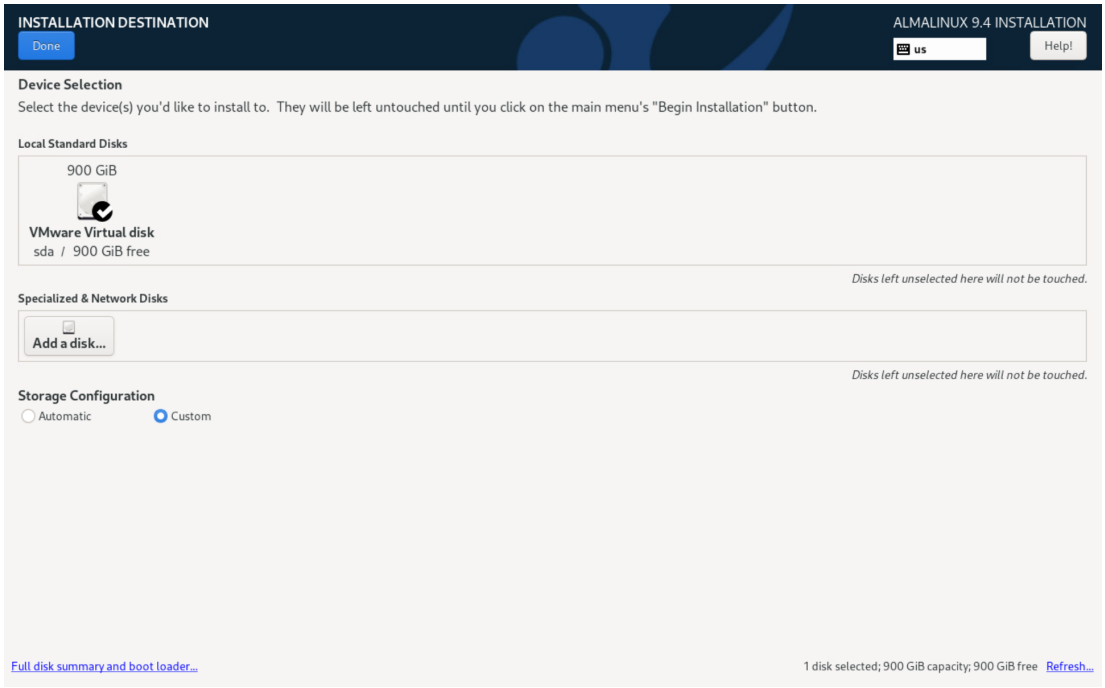
Use the xfs file system for partitioning.

Partition */srv* is a data partition.

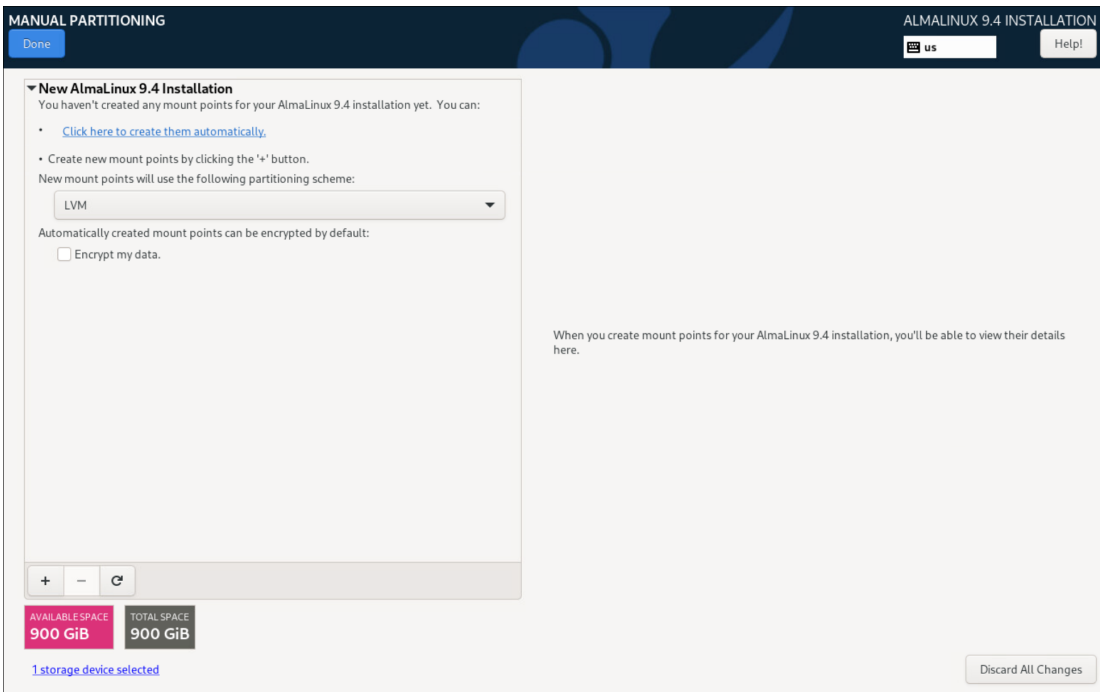
If there is only a little disk space, you can decrease the size of the */home* and */* partitions by 10-20 GB.

A.4.3.2 Partitioning the destination disk automatically

1. In **INSTALLATION DESTINATION**, start manual partitioning:
   a. Select the hard disk.
   b. Select **Select Storage Configuration, Custom**.
   c. Select **Done**.



2. Select **Click here to create them automatically**.

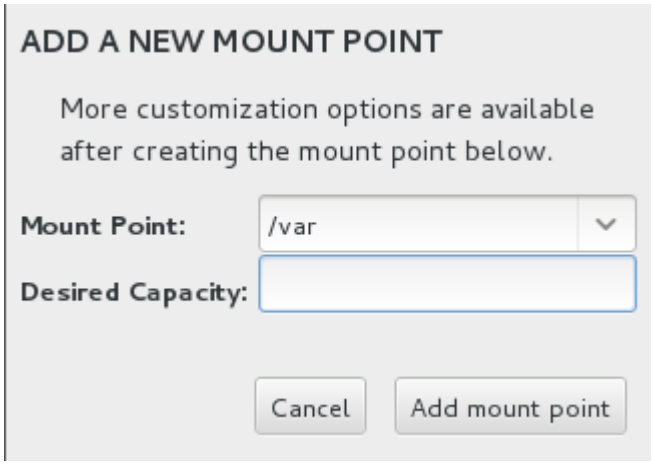


After creating the automatic partitions, you need to modify the partition manually in the next steps.

3. Modify the **/home** partition.
   a. Select the */home* partition.
   b. Under **Desired Capacity**, set the size of the home partition (*/home*) to **`50 GiB`**.
   c. Set the **File System** to **`ext4`**.
   d. Select **Update Settings**.

4. Create the */var* partition:
   a. Select the plus (**+**) icon.

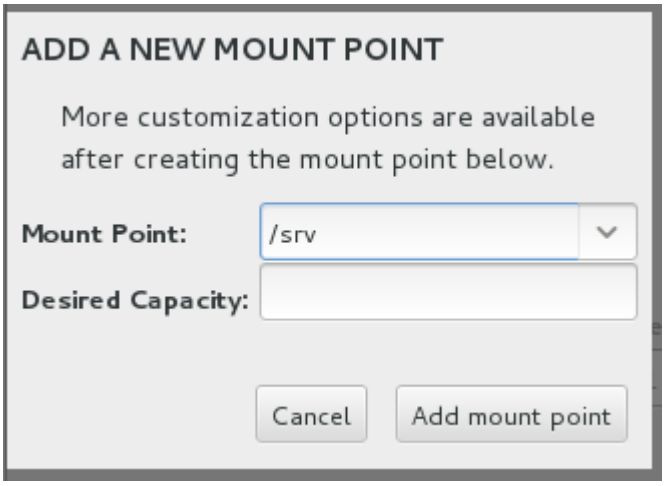
      The **ADD A NEW MOUNT POINT** dialog appears.



   b. In **Mount Point**, type */var*
   c. Under **Desired Capacity**, set the size of the */var* partition by typing **`50 GiB`**.
   d. Select **Add mount point**.
5. Select **/boot**.
   a. Under **Desired Capacity**, set the size of the */boot* partition by typing **`500 MiB`**.
   b. Select **Update Settings**.
6. Select **/**.
   a. Under **Desired Capacity**, set the size of the root partition (/) by typing **`50 GiB`**.
   b. Select **Update Settings**.
7. Select **swap**.
   a. Under **Desired Capacity**, set the size of the swap to the size that corresponds to RAM + 2 GB.
   b. Select **Update Settings**.

8. Create the `/srv` partition:
   a. Select the plus (**+**) icon.

      The **ADD A NEW MOUNT POINT** dialog appears.



   b. In **Mount Point**, type `/srv`
   c. Under **Desired Capacity**, use nearly all the available server space (indicated in the pink box) for the `/srv` partition by typing, for example, **`284 GiB`**.

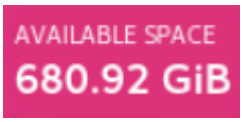


      Figure 2 Example of available disk space

   d. Select **Add mount point**.
9. Select **Done**.
10. In the window listing the partitions, check that the partitions are defined as described in Recommended partitioning settings (page 77).
11. Select **Done > Accept Changes**.

A.4.3.3 Partitioning the destination disk manually

1. On the installation summary page, select **Destination Installation**.
2. To select the destination disk for the AlmaLinux installation, select the **Disk** icon.

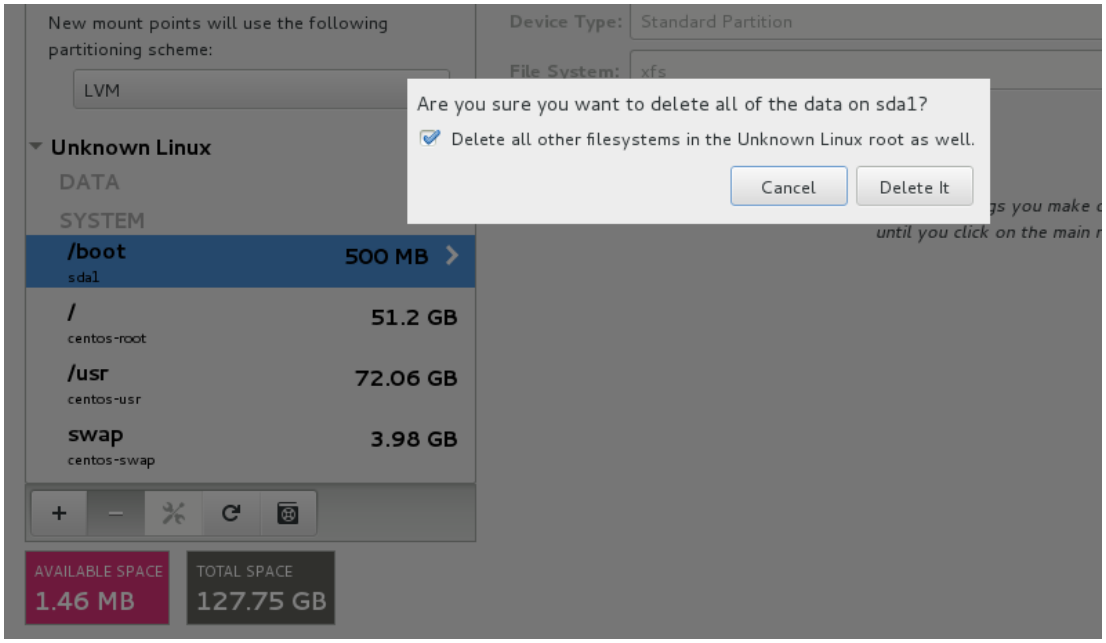
   Once selected, a check mark appears on the icon.
3. Select **Storage configuration > Custom**.

   For recommended settings, see Recommended partitioning settings (page 77).
4. Follow the instructions to create new partitions, or, if needed, to re-use or delete existing partitions.

A.4.3.3.1 Deleting existing partitions

If you do not want to use the existing partitions, you must delete them to provide disk space for your installation.

1. Select the arrow to the left of the drive name you want to modify to expand the partitioning scheme.
2. Select a partition to delete.
3. Select a minus sign (-) icon to delete the partition.
4. On the pop-up window, check **Delete all other filesystems....** and select **Delete it**.



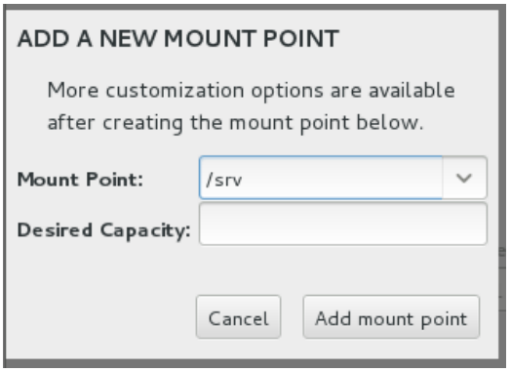
A.4.3.3.2 Creating new partitions

Vaisala recommends the LVM partition scheme.

1. If the */home* partition exists, delete it by selecting the minus (-) icon.
2. Select the plus (+) icon to add partitions.

   Do this 4 times, once for each partition.

3. For each new directory, do the following:



   a. From the **Mount Point** menu, select the directory.
   b. Go to **ADD A NEW MOUNT POINT > Desired Capacity**, and type the value recommended in Recommended partitioning settings (page 77).
   c. Select **Add mount point**.

4. Create the */srv* partition:
   a. In the **Mount Point** field, type */srv*.

      Type a number larger than the remaining data size. For example: **9999999999**.

   b. Select **Add mount point**.

5. One at a time, select each partition, and modify the value in the **Desired Capacity** field with recommended values.

   For **File System Type**, you can select either **EXT4** or **xfs**.

6. Select **Done > Accept changes** to finish partitioning.

When you have completed partitioning, do one of the following:

- If you are doing a manual installation, go to Starting the installation (page 84).
- If you are doing an automatic installation, go back to Installing AlmaLinux automatically (page 64).

A.4.3.3.3 Re-using existing partitions

If your disk has an operating system installed, the partitioning scheme list is displayed.

1. To expand the partitioning scheme, select the arrow to the left of the drive name you want to re-use.
2. In the partition window, for each partition shown in the left pane, select the partition, and enter the name shown in the **Mount Point** field.

   For the **swap** partition, you do not need to enter the mount point name, but you still need to perform steps 3 and 4.

3. Check the **Reformat** check box next to the **File System** drop-down list.
4. Select **Update Settings**.

5. When you have updated the settings for all the partitions, select **Done**.
6. Select **Accept Changes** to return to the installation summary page.

A.4.4 Starting the installation

Before starting the installation, make sure you have your root password and user account information.

1. In the lower right corner of the installation summary page, select **Begin installation**.

   The user settings configuration page appears.
2. While the installation process is in progress and before the end of the installation, configure the `root` password.
3. When installation status shows complete, select **Reboot** and remove the installation media.

   The installation takes 20 ... 30 minutes.
4. If the server does not reboot automatically, use the power button to power cycle the system.
5. If on the first boot you see the prompt window **Accept the License Information**, in the initial setup window:
   a. Select **License Information**.
   b. Check the **I accept the license agreement** box.
   c. Select **Done**.
   d. Select **Finish configuration**.

   Login screen is displayed.
6. Disable monitor negotiation.
7. The first time you login to each new account, follow the series of windows to verify your keyboard and localization settings.
   a. Select **Next** until you get to the thank you screen.
   b. Select **Start using**.
8. Log out of the user account to continue with the installation.

More information

- Disabling monitor negotiation (page 84)

A.4.5 Disabling monitor negotiation

During manual operating system installations, Vaisala recommends disabling monitor negotiation to ensure that the server recognizes the monitors.

1. In the */etc/default/grub* file, add **nomodeset**:
   a. Log in as **admin** user.
   b. Type:

```
sudo  gedit /etc/default/grub
```

   c. In the **GRUB_CMDLINE_LINUX** line, after "**quiet**", add **nomodeset**.
   d. Save your changes.
2. To update the configuration file, run the following script as **admin** user:

```
sudo cd /boot/grub2/
sudo grub2-mkconfig -o grub.cfg
```

A.4.6 Configuring time sync with chronyd

You can configure your machine to time sync with another machine using **chronyd**.

1. In the */etc/crony.conf* file, update the lines that start with the word **server** by removing the default server lines and adding your own. For example:

```
# configure the servers for synchronization using ip address or name
    server 198.102.75.10 iburst
    server 0.centos.pool.ntp.org iburst
```

2. If **chronyd** is already running and you would like changes to take effect, use the following command:

```
#systemctl restart chronyd.service
```

3. If you would like NTP to start automatically on restart, type:

```
#systemctl enable chronyd.service
```

This takes effect after the next reboot. To start without rebooting, type:

```
#systemctl start chronyd.service
```

The system takes 15 minutes to sync the time. If the times are more than 10 minutes apart, NTP assumes there is an error and does not change the time.

4. To check on the status of `chronyd`, type:

```
# chronyd sources -v
```

The first character before the server host is * when it is time synced.

A.4.7 Rebooting the system

1. When the installation is complete, select **Reboot** to reboot the system.
2. Depending on your system bios boot sequence setting, you may need to remove the installation media right after you see the system shutdown complete window flash by in order to boot using the hard drive.

A.4.8 Logging in with your user account

After rebooting, the login window shows the user account you created.

1. Select your user account, and enter your password in the text box.
2. Select **Sign in**.

   The first time you log in to each new user account, you are asked to set some initialization settings. The default settings are normally properly set during the installation process, and no setting changes should be required.
3. In the **Welcome** window, select your language, and select **Next**.
4. In the **Input Sources** window, verify your source, and select **Next**.
5. In the **On-line Accounts** window, select **Next**.
6. In the **Thank you** window, select **Start using AlmaLinux**.
7. Read the **GNOME Help** window and press **X** in the upper right corner to close the window.

   The installation and initialization process for AlmaLinux is complete.

Appendix B. IRIS Diagnostic Utilities

B.1 ps_iris command

Use the **`ps_iris`** command to list currently active IRIS, antenna, and utility processes, including information about their owner UID, PID, time start time, and total CPU time.



To stop a process, use the **`PID`** as an argument to the **`kill`** command.

For example:

```
Detached Processes:
   USER     GROUP PID  PPID  NI PRI %CPU TIME %MEM    VSZ COMMAND
   operator users 3353   1   0  19  0.0  0:02  0.0 168216 server IRIS_SERVER
   operator users 3355   1   4  15  0.0  0:00  0.0 142236 sserver IRIS_SSERVER
   operator users 3399   1  -8  27  0.0  0:49  0.0 136788 ingfio IRIS_INGFIO
   operator users 3407   1   4  15  0.0  0:00  0.0 136768 network IRIS_NETWORK
   operator users 3411   1   8  11  0.4  7:17  0.0 143124 product IRIS_PRODUCT
   operator users 3413   1   8  11  0.0  0:00  0.0 157800 reingest
IRIS_REINGEST
   operator users 3415   1   4  15  0.0  0:00  0.1 180620 output IRIS_OUTPUT001
   operator users 3418   1   4  15  0.0  0:01  0.0 156556 output IRIS_OUTPUT002
   operator users 3420   1   0  19  0.0  0:02  0.0 136776 input IRIS_INPUT01
   operator users 3423   1   0  19  0.0  0:09  0.0 138996 watchdog
IRIS_WATCHDOG
   operator users 23970  1  -8  27  0.0  0:08  0.0 142164 ingest IRIS_INGEST
```

```
Antenna Processes:
   USER     GROUP  PID  PPID  NI PRI %CPU   TIME %MEM    VSZ COMMAND
   operator users  1756   1    0   19  0.0  0:04  0.0 115676 ant_logd ANT_LOGD
   operator users  1789   1   -15  34  0.0  0:51  0.0 115684 ant_rcvd ANT_RCVD
   operator users  1793  1789 -15  34  0.0  1:10  0.0 115684 ant_rcvd ANT_RCVD
   operator users  1823   1   -15  34  0.0  1:08  0.0 115680 ant_xmtd ANT_XMTD
```

```
Stand-alone Utilities:
   USER     GROUP      PID  PPID  NI PRI %CPU   TIME %MEM    VSZ COMMAND
   radarop  radarop  23933 23923   0  19  0.0   0:00  0.0 116244 audio
iris_audio
   operator users     4321  4319   4  15  0.0   0:00  0.0  12636 clntRecv
CLNT_RECV_WINDOW -pipe 8
   radarop  radarop  23923  4163   0  19  0.0   0:04  0.0 189464 iris
   radarop  radarop  23934 23923   0  19  0.0   0:00  0.0 116236 iris_clnt_rcv
7 1073741826
   operator users     3330     1   0  19  4.6  67:30  0.0 699324 /rcp8 -
console /dev/null
   operator users     2021     1   0  19  9.4 138:57  0.4 796880 /rvp10 -
daemon
   operator users     2297  2021   -  50 12.0 176:43  0.3 275560 rvp10proc
RVP10_PROC-0
   operator users     2347  2021   -  50 11.8 172:44  0.3 275556 rvp10proc
RVP10_PROC-1
```

B.2 show_iris command

Use the **show_iris** command to show information about the IRIS process: When it started, the present state of semaphores and event flags, and the current inventory of in-use products.

The **show_iris** command also provides command line options for in–use bits. For more information, type **show_iris -help**.

```
$ show_iris
IRIS Activity on 'hot' at: 09:52:52 17 SEP 1999
IRIS V7.11 was started at 16:19:38 16 SEP 1999 by 'joe'.
Manual startup from TTY:'/dev/tty' ; Restarts:1
Features License: 00004001-000101-WAHRMA-01-Y9ANHF
Products License: 000007FF-000101-WAHRMA-03-WFW4KR
```

```
Present states of Semaphores...

PROCESS CONTROL: FREE (ID: 5833)    PROCESS MODES: FREE (ID: 5826)
TASK SCHEDULE: FREE (ID: 5834)    PRODUCT SCHEDULE: FREE (ID: 5831)
INGEST DIRECTORY: FREE (ID: 5831)    PRODUCT DIRECTORY: FREE (ID: 5849)
DEVICE TABLE: FREE (ID: 5852)    MODE SWITCH TABLE: FREE (ID: 5834)
ARCHIVE DIRECTORY: FREE (ID: 5834)    ERROR LOG: FREE (ID: 5834)

Present states of Event Flags...
RTDISP: CLEAR    INGEST: CLEAR
INGFIO: CLEAR    INGFIO MAPPING: SET
INGFIO WAITING: SET    WATCHDOG: CLEAR
PRODUCT: CLEAR    REINGEST: CLEAR
NETWORK: CLEAR    NORDRAD: CLEAR
GLOBAL MAPPED: SET
```

```
Event Flags SET for Output Processes: 7 8
Event Flags SET for Network Child Processes: 1 2 3 4 5 6 7 8 9 10 11 12 13 14
15 16
Checking INGEST inventory for in-use files:
Total files checked: 92, total in use: 0.
Checking PRODUCT inventory for in-use files:
Total files checked: 260, total in use: 0.
```

```
======= Product Inventory Contents =======
Prod Type        Count        Size(Mb)        Kept Count        Kept Size
PPI              0             0.00             0             0.00
RHI              0             0.00             0             0.00
CAPPI          159            92.06            21            60.92
Cross Section    0             0.00             0             0.00
Echo Tops        0             0.00             0             0.00
Tracking         0             0.00             0             0.00
Hourly Rainfall  0             0.00             0             0.00
N Hours Rainfall 0             0.00             0             0.00
Vol. Vel. Proc.  0             0.00             0             0.00
Vert.Int. Liquid 0             0.00             0             0.00
Wind Shear       0             0.00             0             0.00
Warning          1             0.01             0             0.01
Real Time PPI    0             0.00             0             0.00
Real Time RHI    0             0.00             0             0.00
Raw Data        73            52.35            73            52.35
Max with panels  0             0.00             0             0.00
User Map         0             0.00             0             0.00
User Section     0             0.00             0             0.00
User Other       0             0.00             0             0.00
Status          25             0.06             0             0.00
Shear Line       0             0.00             0             0.00
Horizontal Wind  0             0.00             0             0.00
Beam Pattern     0             0.00             0             0.00
Text             0             0.00             0             0.00
Forecast         0             0.00             0             0.00
Multi-Doppler    2            15.36             2            15.36
Image            0             0.00             0             0.00
Composite        0             0.00             0             0.00
LLWAS            0             0.00             0             0.00
                260          159.84 Mb          97          128.65 Mb
```

B.3 sigmet_env Command

Use **`sigmet_env`** to test or troubleshoot items associated with an IRIS installation.

To sue the command, log in as a normal IRIS user, run **`sigmet_env`**. The **`sigmet_env`** command checks the following:

- That all the IRIS operators and observers are in the */etc/users* file.
- That all IRIS environment variables that point to directories are defined and the directory exists, and the directory can be read and written as required.
- For obvious bad file names in the saved menu directory.
- That IRIS executable files which require the **`set-UID-on-execute`** bit set are set with the correct UID.
- The RDA (RVP/RCP) environment.

The following example shows a case with a bad file name of *.TSC*.

```
$ sigmet_env
Checking IRIS_OPERATORS list...
Checking IRIS_OBSERVERS list...
Checking installation directories...
Checking configuration directories...
Checking data directories...
Checking file names in IRIS_MENU...
Bad menu filename: '/etc/vaisala/irisrda/menu/.TSC'
Checking root file ownerships...

Errors Detected -- Please Check Printout
```

Appendix C. Alternative Configurations

C.1 Defining the operator list in the startup file

Most environments can function with **radarop** and **observer** users without any further definitions. If you wish to manage named users, follow the instructions below.

The */etc/vaisala/irisrda/profile.conf* file defines some of the base configuration, including the lists of users who can operate IRIS fully, and who can observe its operation but not make any changes.



Every IRIS user must share group access to files owned by the operator by being a member of the users group.

1. Edit the file and change these as needed.

```
operators='radarop operator john george mary root'
observers='observer'
```

2. Check your environment by typing:

```
$ env | grep IRIS
```

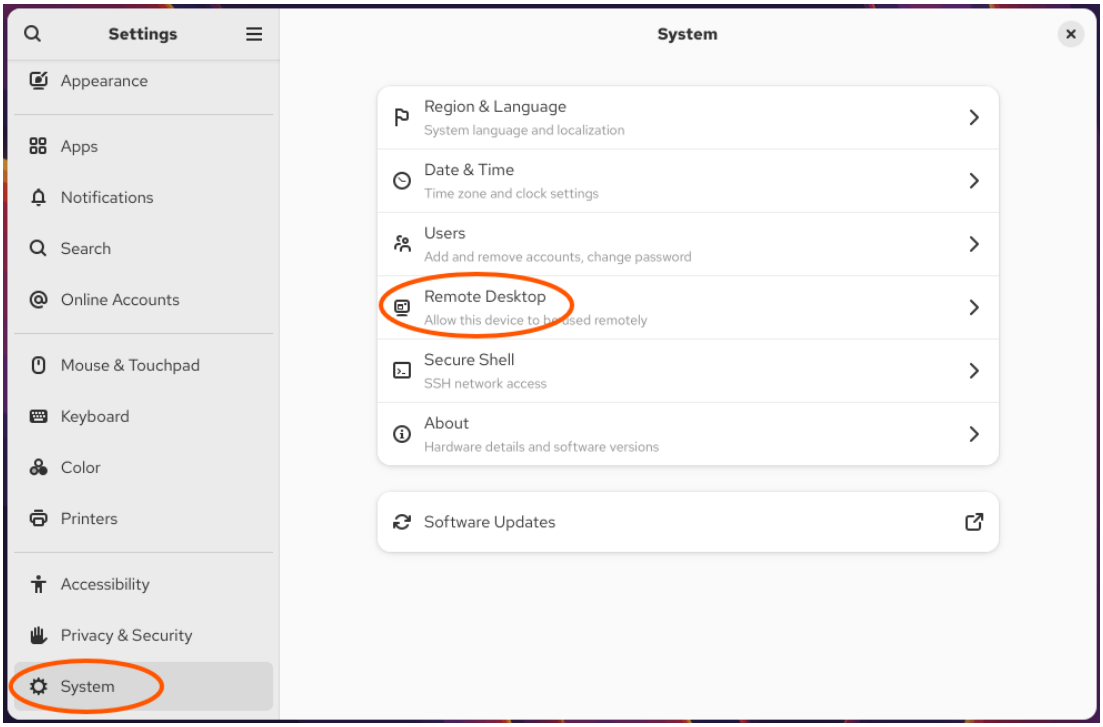
C.2 Configuring remote desktop

AlmaLinux 10.1 has the remote desktop installed by default. Follow this procedure to enable it.

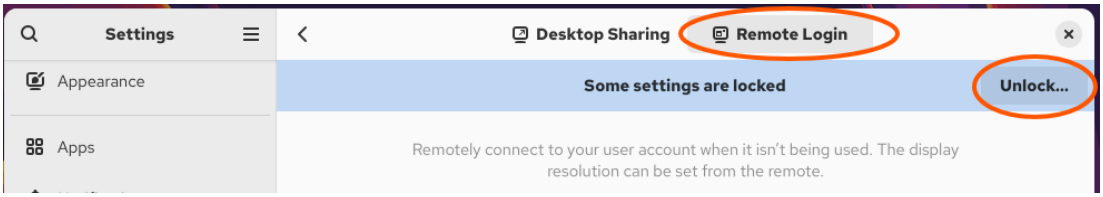
1. Log in as **admin**.
2. Add a rule to the firewall to allow traffic to port 3389 by running the following commands:

```
sudo firewall-cmd --add-port=3389/tcp --permanent
sudo firewall-cmd --add-port=3389/udp --permanent
sudo firewall-cmd --reload
```

3. Open the AlmaLinux settings: in the top right corner, select the "**power**" button, and then the "**gear**" (⚙) button.
4. In the **Settings** window, on the bottom left, select **System**, and then **Remote Desktop**.



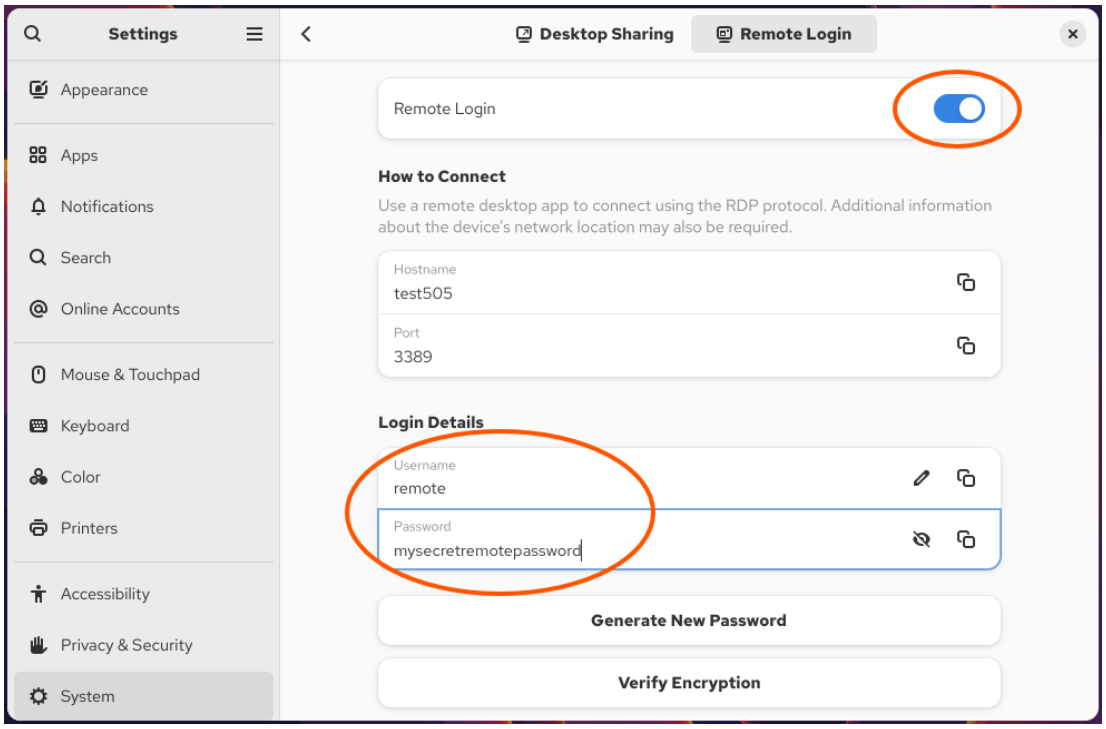
5. In the next view, select **Remote Login** and then **Unlock...**



6. Give the admin user password.
7. Use the **Remote Login** toggle to turn on the remote login.

8. In the **Login Details** field, set the username and password for the remote connection.

> **NOTICE!** Do not use any existing username or password. This username and password are needed to login to remote desktop, and it does not allow access to the system itself.



9. Close the **Settings** window.
10. Open the terminal and restart the remote desktop service with the following command:

```
sudo systemctl restart gnome-remote-desktop
```

Now you can log in remotely to the system using the hostname, port, username, and password given in the remote desktop settings. When the login is successful, you see the AlmaLinux login screen. From there, you can log in using the normal usernames and passwords.

> The remote desktop may take a long time to establish the connection. After the connection has been made, using the remote desktop is normally quite smooth.

Warranty

For warranty terms and conditions and the warranty claim process, see vaisala.com/warranty.

Note that warranty coverage may not apply if the product is damaged due to normal wear and tear, exceptional operating conditions, negligent handling or installation, or unauthorized modifications. See the applicable supply contract or Conditions of Sale for details of the warranty for each product.

Technical support



You can contact Vaisala technical support at vaisala.my.site.com/myvaisala or helpdesk@vaisala.com. You can find all our support channels at vaisala.com/support.

When contacting technical support, provide the following as applicable:

- Product name, model, and serial number
- Software/Firmware version
- Name and location of the installation site
- Name and contact information of a technical person who can provide further information
- Diagnostics package for the application

If applicable, also provide the following details:

- What failed (what worked / did not work)?
- Where did it fail (location and environment)?
- When did it fail (date, immediately / after a while / periodically / randomly)?
- How many failed (only one defect / other same or similar defects / several failures in one unit)?
- What was done when the failure was noticed?
- What was connected to the product and to which connectors?
- What is the input power source type, voltage, and what else (such as lighting, heaters, and motors) was connected to the same power output?
- Are all parts connected and grounded properly? Take a photo to help the troubleshooting.

Recycling



Recycle all applicable material according to local regulations.

VAISALA